

# ***HS-100 / HS-100W***

***Parental Control Gateway***

## ***User's Guide***

Version 3.62

10/2005



# Copyright

## **Copyright © 2004 by ZyXEL Communications Corporation.**

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## **Disclaimer**

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice.

This publication is subject to change without notice.

## **Trademarks**

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a CLASS B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

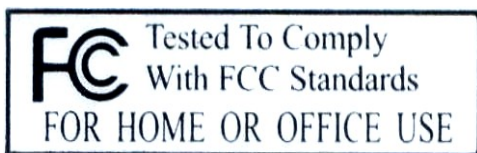
Consult the dealer or an experienced radio/TV technician for help.

## Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Certifications

1. Go to [www.zyxel.com](http://www.zyxel.com).
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.



## Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

### **Caution**

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

### **Note**

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.



## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### NOTE

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.



### Online Registration



---

Register your product online at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

---

# Customer Support

When you contact your customer support representative please have the following information ready:

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE <sup>1</sup> FAX <sup>1</sup>	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	<a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a>  <a href="mailto:sales@zyxel.com.tw">sales@zyxel.com.tw</a>	+886-3-578-3942  +886-3-578-2439	<a href="http://www.zyxel.com">www.zyxel.com</a> <a href="http://www.europe.zyxel.com">www.europe.zyxel.com</a> <a href="ftp://ftp.zyxel.com">ftp.zyxel.com</a> <a href="ftp://ftp.europe.zyxel.com">ftp.europe.zyxel.com</a>	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	<a href="mailto:support@zyxel.com">support@zyxel.com</a>  <a href="mailto:sales@zyxel.com">sales@zyxel.com</a>	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	<a href="http://www.us.zyxel.com">www.us.zyxel.com</a>  <a href="ftp://ftp.us.zyxel.com">ftp.us.zyxel.com</a>	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	<a href="mailto:support@zyxel.de">support@zyxel.de</a>  <a href="mailto:sales@zyxel.de">sales@zyxel.de</a>	+49-2405-6909-0 +49-2405-6909-99	<a href="http://www.zyxel.de">www.zyxel.de</a>	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	<a href="mailto:info@zyxel.fr">info@zyxel.fr</a>	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	<a href="http://www.zyxel.fr">www.zyxel.fr</a>	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	<a href="mailto:support@zyxel.es">support@zyxel.es</a>  <a href="mailto:sales@zyxel.es">sales@zyxel.es</a>	+34 902 195 420 +34 913 005 345	<a href="http://www.zyxel.es">www.zyxel.es</a>	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	<a href="mailto:support@zyxel.dk">support@zyxel.dk</a>  <a href="mailto:sales@zyxel.dk">sales@zyxel.dk</a>	+45 39 55 07 00 +45 39 55 07 07	<a href="http://www.zyxel.dk">www.zyxel.dk</a>	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	<a href="mailto:support@zyxel.no">support@zyxel.no</a>  <a href="mailto:sales@zyxel.no">sales@zyxel.no</a>	+47 22 80 61 80 +47 22 80 61 81	<a href="http://www.zyxel.no">www.zyxel.no</a>	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	<a href="mailto:support@zyxel.se">support@zyxel.se</a>  <a href="mailto:sales@zyxel.se">sales@zyxel.se</a>	+46 31 744 7700 +46 31 744 7701	<a href="http://www.zyxel.se">www.zyxel.se</a>	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	<a href="mailto:support@zyxel.fi">support@zyxel.fi</a>  <a href="mailto:sales@zyxel.fi">sales@zyxel.fi</a>	+358-9-4780-8411 +358-9-4780 8448	<a href="http://www.zyxel.fi">www.zyxel.fi</a>	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

<sup>1</sup> “+” is the (prefix) number you enter to make an international telephone call.

# Table of Contents

Getting Started.....	I
Chapter 1 Getting to Know Your HomeSafe .....	1-1
1.1 HomeSafe Parental Control Gateway Overview .....	1-1
1.2 HomeSafe Features .....	1-1
1.3 Applications for the HomeSafe .....	1-5
Chapter 2 Introducing the Web Configurator .....	2-1
2.1 Web Configurator Overview .....	2-1
2.2 Accessing the HomeSafe Web Configurator .....	2-1
2.3 Step 1 : System Administrator Password Setup.....	2-2
2.4 Step 2 : WLAN Setup.....	2-2
2.5 Step 3 : Internet Configuration Setup .....	2-5
2.6 Step 4 : Parental Control Wizard.....	2-8
2.7 Step 5 : Content Filter Service Activation .....	2-18
2.8 Accessing the Internet via the HomeSafe Gateway .....	2-19
2.9 Accessing the HomeSafe Web Configurator .....	2-20
2.10 Resetting the HomeSafe .....	2-21
2.11 HomeSafe Main Menu .....	2-21
Chapter 3 Connection Wizard.....	3-1
3.1 Connection Wizard Overview .....	3-1
3.2 Connection Wizard : General Setup and System Name .....	3-1
3.3 Connection Wizard: Screen 2.....	3-2
3.4 Connection Wizard : Screen 3.....	3-3
3.5 Connection Wizard : Screen 4.....	3-4
3.6 Connection Wizard : Screen 5.....	3-8
3.7 Basic Setup Complete .....	3-11
System, LAN, WLAN and WAN .....	II
Chapter 4 System Screens.....	4-1
4.1 System Overview .....	4-1
4.2 Configuring General Setup .....	4-1
4.3 Dynamic DNS .....	4-2
4.4 Configuring Dynamic DNS.....	4-2
4.5 Configuring Password .....	4-4
4.6 Configuring Time Setting .....	4-4
Chapter 5 LAN Screens .....	5-1
5.1 LAN Overview .....	5-1
5.2 DHCP Setup.....	5-1
5.3 LAN TCP/IP .....	5-1
5.4 Any IP .....	5-2
5.5 Configuring IP.....	5-4
5.6 Configuring Static DHCP .....	5-6
5.7 Configuring IP Alias.....	5-7
Chapter 6 Wireless Configuration and Roaming.....	6-1

6.1	Wireless LAN Overview .....	6-1
6.2	Wireless LAN Basics .....	6-3
6.3	Configuring Wireless .....	6-4
6.4	Configuring Roaming .....	6-5
Chapter 7 Wireless Security .....		7-1
7.1	Wireless Security Overview.....	7-1
7.2	Security Parameters Summary .....	7-3
7.3	WEP Overview .....	7-3
7.4	Configuring WEP Encryption.....	7-5
7.5	Introduction to WPA.....	7-6
7.6	Configuring WPA-PSK Authentication.....	7-8
7.7	Wireless Client WPA Supplicants .....	7-9
7.8	Configuring WPA Authentication .....	7-10
7.9	802.1x Overview .....	7-11
7.10	Dynamic WEP Key Exchange .....	7-12
7.11	Configuring 802.1x and Dynamic WEP Key Exchange .....	7-12
7.12	Configuring 802.1x and Static WEP Key Exchange .....	7-13
7.13	Configuring 802.1x .....	7-16
7.14	MAC Filter.....	7-17
7.15	Introduction to Local User Database .....	7-19
7.16	Configuring Local User Database .....	7-19
7.17	Introduction to RADIUS.....	7-20
7.18	Configuring RADIUS.....	7-21
Chapter 8 WAN Screens.....		8-1
8.1	WAN Overview .....	8-1
8.2	TCP/IP Priority (Metric) .....	8-1
8.3	Configuring Route.....	8-1
8.4	Configuring WAN ISP .....	8-2
8.5	Configuring WAN IP.....	8-6
8.6	Configuring WAN MAC .....	8-8
8.7	Traffic Redirect .....	8-9
8.8	Configuring Traffic Redirect.....	8-10
SUA/NAT and Static Route.....		III
Chapter 9 Network Address Translation (NAT) Screens .....		9-1
9.1	NAT Overview .....	9-1
9.2	Using NAT.....	9-4
9.3	SUA Server.....	9-4
9.4	Configuring SUA Server.....	9-6
9.5	Configuring Address Mapping.....	9-7
9.6	Trigger Port Forwarding .....	9-9
9.7	Configuring Trigger Port Forwarding .....	9-10
Chapter 10 Static Route Screens .....		10-1
10.1	Static Route Overview.....	10-1
10.2	Configuring IP Static Route.....	10-1

UPnP, Parental Control and Firewall .....	IV
Chapter 11 UPnP .....	11-1
11.1 Universal Plug and Play Overview.....	11-1
11.2 UPnP and ZyXEL.....	11-1
11.3 Configuring UPnP .....	11-2
11.4 Installing UPnP in Windows Example .....	11-2
11.5 Using UPnP in Windows XP Example .....	11-4
Chapter 12 Parental Control .....	12-1
12.1 Parental Control Overview .....	12-1
12.2 Parental Control Logins.....	12-1
12.3 Parental Control Application.....	12-2
12.4 Configuring Parental Control .....	12-3
12.5 Parental Control Group Edit Filter .....	12-6
12.6 Parental Control Group Edit Configuration.....	12-7
12.7 Customizing Keyword Blocking URL Checking .....	12-13
12.8 Parental Control Edit.....	12-13
12.9 Parental Control Bypass List.....	12-18
Chapter 13 Firewall.....	13-1
13.1 Introduction .....	13-1
13.2 Firewall Settings Screen.....	13-2
13.3 The Firewall, NAT and Remote Management .....	13-3
13.4 Services.....	13-4
Remote Management.....	V
Chapter 14 Remote Management Screens.....	14-1
14.1 Remote Management Overview .....	14-1
14.2 Configuring WWW .....	14-2
14.3 Configuring Telnet.....	14-3
14.4 Configuring TELNET .....	14-3
14.5 Configuring FTP.....	14-4
14.6 SNMP.....	14-5
14.7 Configuring DNS .....	14-9
14.8 Configuring Security .....	14-10
Logs and Maintenance .....	VI
Chapter 15 Centralized Logs.....	15-1
15.1 View Log.....	15-1
15.2 Log Settings.....	15-2
Chapter 16 Maintenance.....	16-1
16.1 Maintenance Overview .....	16-1
16.2 Status Screen.....	16-1
16.3 DHCP Table Screen .....	16-3
16.4 Any IP Table.....	16-4
16.5 Association List.....	16-4
16.6 F/W Upload Screen.....	16-5
16.7 Configuration Screen .....	16-6
16.8 Restart Screen.....	16-9

SMT General Configuration.....	VII
Chapter 17 Introducing the SMT.....	17-1
17.1 SMT Introduction.....	17-1
17.2 Navigating the SMT Interface.....	17-2
17.3 Changing the System Password.....	17-4
Chapter 18 Menu 1 General Setup.....	18-1
18.1 General Setup .....	18-1
18.2 Procedure To Configure Menu 1 .....	18-1
Chapter 19 Menu 2 WAN Setup.....	19-1
19.1 Introduction to WAN.....	19-1
19.2 WAN Setup.....	19-1
Chapter 20 Menu 3 LAN Setup.....	20-1
20.1 LAN Setup.....	20-1
20.2 Protocol Dependent Ethernet Setup.....	20-1
20.3 TCP/IP Ethernet Setup and DHCP.....	20-1
20.4 Wireless LAN Setup .....	20-5
Chapter 21 Internet Access.....	21-1
21.1 Introduction to Internet Access Setup .....	21-1
21.2 Ethernet Encapsulation.....	21-1
21.3 Configuring the PPTP Client.....	21-2
21.4 Configuring the PPPoE Client .....	21-3
21.5 Basic Setup Complete.....	21-4
Chapter 22 Remote Node Configuration.....	22-1
22.1 Introduction to Remote Node Setup .....	22-1
22.2 Remote Node Profile Setup.....	22-1
22.3 Edit IP.....	22-5
22.4 Remote Node Filter .....	22-6
Chapter 23 Static Route Setup .....	23-1
23.1 IP Static Route Setup.....	23-1
Chapter 24 Dial-in User Setup.....	24-1
24.1 Dial-in User Setup.....	24-1
Chapter 25 Network Address Translation (NAT) .....	25-1
25.1 Using NAT .....	25-1
25.2 Applying NAT .....	25-1
25.3 NAT Setup.....	25-2
25.4 Configuring a Server behind NAT .....	25-6
25.5 General NAT Examples.....	25-7
25.6 Configuring Trigger Port Forwarding.....	25-12
Chapter 26 Enabling the Firewall .....	26-1
26.1 Remote Management and the Firewall.....	26-1
26.2 Access Methods.....	26-1
26.3 Enabling the Firewall.....	26-1
SMT Advanced Management .....	VIII
Chapter 27 Filter Configuration .....	27-1

27.1	Introduction to Filters .....	27-1
27.2	Configuring a Filter Set .....	27-3
27.3	Example Filter .....	27-9
27.4	Filter Types and NAT .....	27-11
27.5	Firewall Versus Filters .....	27-12
27.6	Applying a Filter.....	27-12
Chapter 28	SNMP Configuration.....	28-1
28.1	About SNMP .....	28-1
28.2	Supported MIBs .....	28-2
28.3	SNMP Configuration.....	28-2
28.4	SNMP Traps .....	28-3
Chapter 29	System Security.....	29-1
29.1	System Security.....	29-1
Chapter 30	System Information and Diagnosis .....	30-1
30.1	System Status .....	30-1
30.2	System Information .....	30-3
30.3	Log and Trace .....	30-4
30.4	Diagnostic.....	30-6
Chapter 31	Firmware and Configuration File Maintenance .....	31-1
31.1	Filename Conventions .....	31-1
31.2	Backup Configuration.....	31-2
31.3	Restore Configuration.....	31-4
31.4	Uploading Firmware and Configuration Files.....	31-5
Chapter 32	System Maintenance.....	32-1
32.1	Command Interpreter Mode .....	32-1
32.2	Call Control Support.....	32-2
32.3	Time and Date Setting.....	32-4
Chapter 33	Remote Management.....	33-1
33.1	Remote Management.....	33-1
Chapter 34	Call Scheduling .....	34-1
34.1	Introduction to Call Scheduling .....	34-1
Appendices and Index .....		IX
Appendix A Troubleshooting .....		A-1
Appendix B PPPoE.....		B-1
Appendix C PPTP .....		C-1
Appendix D Log Descriptions.....		D-1
Appendix E Setting up Your Computer's IP Address.....		E-1
Appendix F Wireless LAN and IEEE 802.11 .....		F-1
Appendix G Wireless LAN With IEEE 802.1x.....		G-1
Appendix H Types of EAP Authentication .....		H-1
Appendix I Antenna Selection and Positioning Recommendation .....		I-1
Appendix J Brute-Force Password Guessing Protection .....		J-1
Appendix K Triangle Route.....		K-1
Appendix L Index .....		L-1





# List of Figures

Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem .....	1-5
Figure 1-2 HomeSafe Parental Control Gateway Application.....	1-5
Figure 1-3 Wireless LAN Application Example.....	1-6
Figure 2-1 Welcome Menu .....	2-1
Figure 2-2 Wizard Step 1 : Administrator Password .....	2-2
Figure 2-3 Wizard Step 2 : Wireless LAN Setup.....	2-3
Figure 2-4 Wizard Step 2 : Wireless LAN Setup Basic Security .....	2-4
Figure 2-5 Wizard Step 2 : Wireless LAN Setup Extend Security .....	2-5
Figure 2-6 Wizard Step 3 : Internet Access Setup .....	2-5
Figure 2-7 Wizard Step 3 : ISP Parameters .....	2-6
Figure 2-8 Wizard Step 3 : Internet Access Setup .....	2-7
Figure 2-9 Wizard Step 3 : Internet Access Static IP Address Setup .....	2-7
Figure 2-10 Wizard Step 3 : Internet Setup Complete .....	2-8
Figure 2-11 Wizard Step 4 : Parental Control Wizard .....	2-9
Figure 2-12 Wizard Step 4 : Parental Control Time Setup .....	2-10
Figure 2-13 Wizard Step 4 : Create or Edit a Profile.....	2-11
Figure 2-14 Wizard Step 4 : Parental Control Profile Information .....	2-12
Figure 2-15 Wizard Step 4 : Parental Control User Group .....	2-12
Figure 2-16 Wizard Step 4 : Parental Control Time Allowance .....	2-13
Figure 2-17 Wizard Step 4 : Parental Control Application Blocking.....	2-15
Figure 2-18 Wizard Step 4 : Parental Control Summary .....	2-16
Figure 2-19 Content Filtering Lookup Procedure.....	2-17
Figure 2-20 Wizard Step 4 : Content Filter Registration .....	2-18
Figure 2-21 Content Filter Activation in Progress.....	2-18
Figure 2-22 Content Filter Activation in Progress.....	2-18
Figure 2-23 Content Filter Activation Failure .....	2-19
Figure 2-24 Content Filter Setup Complete.....	2-19
Figure 2-25 Password Screen .....	2-20
Figure 2-26 Change Password Screen .....	2-20
Figure 2-27 The MAIN MENU Screen of the Web Configurator .....	2-21
Figure 3-1 Connection Wizard : General Setup.....	3-2
Figure 3-2 Connection Wizard : Wireless LAN Setup.....	3-2
Figure 3-3 Connection Wizard: Wireless LAN Setup: Basic Security .....	3-3
Figure 3-4 Connection Wizard: Wireless LAN Setup: Extend Security .....	3-4
Figure 3-5 Connection Wizard : Ethernet Encapsulation .....	3-5
Figure 3-6 Connection Wizard : PPPoE Encapsulation.....	3-6
Figure 3-7 Connection Wizard : PPTP Encapsulation .....	3-7
Figure 3-8 Connection Wizard : WAN Setup .....	3-10
Figure 3-9 Connection Wizard Finish.....	3-11
Figure 3-10 Connection Wizard Problems .....	3-12
Figure 4-1 SYSTEM : General Setup.....	4-1

Figure 4-2 SYSTEM : DDNS .....	4-3
Figure 4-3 SYSTEM : Password .....	4-4
Figure 4-4 SYSTEM : Time Setting .....	4-5
Figure 5-1 Any IP Example Application.....	5-3
Figure 5-2 LAN : IP .....	5-4
Figure 5-3 LAN : Static DHCP .....	5-6
Figure 5-4 LAN : IP Alias .....	5-7
Figure 6-1 IBSS (Ad-hoc) Wireless LAN .....	6-1
Figure 6-2 Basic Service set .....	6-2
Figure 6-3 Extended Service Set .....	6-2
Figure 6-4 RTS/CTS.....	6-3
Figure 6-5 WLAN : Wireless.....	6-4
Figure 6-6 Roaming Example.....	6-6
Figure 6-7 WLAN : Roaming.....	6-7
Figure 7-1 HomeSafe Wireless Security Levels.....	7-1
Figure 7-2 WLAN : Wireless : No Security .....	7-2
Figure 7-3 WEP Authentication Steps .....	7-4
Figure 7-4 WLAN : Wireless : Static WEP Encryption.....	7-5
Figure 7-5 WPA - PSK Authentication.....	7-7
Figure 7-6 WLAN : Wireless : WPA-PSK.....	7-8
Figure 7-7 WPA with RADIUS Application Example.....	7-10
Figure 7-8 Wireless: WPA.....	7-10
Figure 7-9 WLAN : Wireless : 802.1x and Dynamic WEP.....	7-12
Figure 7-10 WLAN : Wireless : 802.1x and Static WEP.....	7-14
Figure 7-11 WLAN : Wireless: 802.1x.....	7-16
Figure 7-12 WLAN : MAC Address Filter.....	7-18
Figure 7-13 WLAN : Local User Database .....	7-19
Figure 7-14 EAP Authentication .....	7-21
Figure 7-15 WLAN : RADIUS .....	7-22
Figure 8-1 WAN : Route.....	8-1
Figure 8-2 WAN ISP : Ethernet Encapsulation.....	8-2
Figure 8-3 WAN ISP : PPPoE Encapsulation .....	8-4
Figure 8-4 WAN ISP : PPTP Encapsulation .....	8-5
Figure 8-5 WAN : IP.....	8-6
Figure 8-6 WAN : MAC Setup.....	8-8
Figure 8-7 Traffic Redirect WAN Setup.....	8-9
Figure 8-8 Traffic Redirect LAN Setup.....	8-9
Figure 8-9 WAN : Traffic Redirect.....	8-10
Figure 9-1 How NAT Works.....	9-2
Figure 9-2 NAT Application With IP Alias.....	9-3
Figure 9-3 Multiple Servers Behind NAT Example .....	9-6
Figure 9-4 SUA/NAT Setup .....	9-7
Figure 9-5 Address Mapping .....	9-8
Figure 9-6 Address Mapping Edit .....	9-9

Figure 9-7 Trigger Port Forwarding Process: Example .....	9-10
Figure 9-8 Trigger Port.....	9-11
Figure 10-1 Example of Static Routing Topology .....	10-1
Figure 10-2 Static Route.....	10-1
Figure 10-3 Static Route: Edit .....	10-2
Figure 11-1 Configuring UPnP.....	11-2
Figure 12-1 HomeSafe Network User Login.....	12-1
Figure 12-3 User Status Window .....	12-2
Figure 12-4 HomeSafe Parental Control Wireless Gateway Application .....	12-3
Figure 12-5 Parental Control .....	12-4
Figure 12-6 Content Filtering Lookup Procedure.....	12-6
Figure 12-7 Parental Control : Filter .....	12-8
Figure 12-8 Parental Control : Edit .....	12-16
Figure 12-9 Parental Control : Bypass List .....	12-18
Figure 13-1 Firewall: Settings .....	13-2
Figure 13-2 Firewall Rule Directions .....	13-3
Figure 13-3 Firewall: Service .....	13-5
Figure 14-1 Remote Management : WWW.....	14-2
Figure 14-2 Telnet Configuration on a TCP/IP Network.....	14-3
Figure 14-3 Remote Management : Telnet .....	14-4
Figure 14-4 Remote Management : FTP .....	14-5
Figure 14-5 SNMP Management Model .....	14-6
Figure 14-6 Remote Management : SNMP .....	14-8
Figure 14-7 Remote Management : DNS .....	14-9
Figure 14-8 Remote Management : Security.....	14-10
Figure 15-1 View Logs .....	15-1
Figure 15-2 Log Settings .....	15-3
Figure 16-1 Maintenance : Status .....	16-1
Figure 16-2 Maintenance : System Statistics.....	16-2
Figure 16-3 Maintenance : DHCP Table.....	16-3
Figure 16-4 Maintenance : Any IP .....	16-4
Figure 16-5 Maintenance : Association List.....	16-4
Figure 16-6 Maintenance : Firmware Upload.....	16-5
Figure 16-7 Upload Warning .....	16-6
Figure 16-8 Network Temporarily Disconnected .....	16-6
Figure 16-9 Upload Error Message .....	16-6
Figure 16-10 Maintenance : Configuration .....	16-7
Figure 16-11 Configuration : Restore Successful.....	16-8
Figure 16-12 Temporarily Disconnected .....	16-8
Figure 16-13 Configuration Restore Error .....	16-8
Figure 16-14 Factory Defaults.....	16-9
Figure 16-15 Maintenance : System Restart.....	16-9
Figure 17-1 Login Screen .....	17-1
Figure 17-2 SMT Menu Overview .....	17-2

Figure 17-3 SMT Main Menu .....	17-3
Figure 17-4 Menu 23 System Password .....	17-4
Figure 18-1 Menu 1 General Setup .....	18-1
Figure 18-2 Menu 1.1 Configure Dynamic DNS .....	18-3
Figure 19-1 Menu 2 WAN Setup .....	19-1
Figure 20-1 Menu 3 LAN Setup.....	20-1
Figure 20-2 Menu 3.1 LAN Port Filter Setup.....	20-1
Figure 20-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup.....	20-2
Figure 20-4 Physical Network & Partitioned Logical Networks.....	20-4
Figure 20-5 Menu 3.2.1: IP Alias Setup .....	20-4
Figure 20-6 Menu 3.5 Wireless LAN Setup .....	20-5
Figure 20-7 Menu 3.5 Wireless LAN Setup .....	20-7
Figure 20-8 Menu 3.5.1 WLAN MAC Address Filter.....	20-8
Figure 20-9 Menu 3.5 Wireless LAN Setup .....	20-9
Figure 20-10 Menu 3.5.2 Roaming Configuration .....	20-9
Figure 21-1 Menu 4 Internet Access Setup.....	21-1
Figure 21-2 Internet Access Setup (PPTP) .....	21-3
Figure 21-3 Internet Access Setup (PPPoE) .....	21-3
Figure 22-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation.....	22-1
Figure 22-2 Menu 11.1 Remote Node Profile for PPPoE Encapsulation .....	22-3
Figure 22-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation .....	22-4
Figure 22-4 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation.....	22-5
Figure 22-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation).....	22-7
Figure 22-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation) .....	22-7
Figure 22-7 Menu 11.6: Traffic Redirect Setup.....	22-7
Figure 23-1 Menu 12 IP Static Route Setup .....	23-1
Figure 23-2 Menu 12.1 Edit IP Static Route.....	23-1
Figure 24-1 Menu 14- Dial-in User Setup .....	24-1
Figure 24-2 Menu 14.1- Edit Dial-in User .....	24-1
Figure 25-1 Menu 4 Applying NAT for Internet Access.....	25-1
Figure 25-2 Menu 11.3 Applying NAT to the Remote Node.....	25-2
Figure 25-3 Menu 15 NAT Setup .....	25-2
Figure 25-4 Menu 15.1 Address Mapping Sets .....	25-3
Figure 25-5 Menu 15.1.255 SUA Address Mapping Rules .....	25-3
Figure 25-6 Menu 15.1.1 First Set.....	25-4
Figure 25-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	25-5
Figure 25-8 Menu 15.2.1 NAT Server Setup.....	25-6
Figure 25-9 Multiple Servers Behind NAT Example .....	25-7
Figure 25-10 NAT Example 1 .....	25-7
Figure 25-11 Menu 4 Internet Access & NAT Example .....	25-7
Figure 25-12 NAT Example 2 .....	25-8
Figure 25-13 Menu 15.2.1 Specifying an Inside Server.....	25-8
Figure 25-14 NAT Example 3 .....	25-9
Figure 25-15 Example 3: Menu 11.3 .....	25-9

Figure 25-16 Example 3: Menu 15.1.1.1 .....	25-10
Figure 25-17 Example 3: Final Menu 15.1.1 .....	25-10
Figure 25-18 NAT Example 4 .....	25-11
Figure 25-19 Example 4: Menu 15.1.1.1 Address Mapping Rule .....	25-11
Figure 25-20 Example 4: Menu 15.1.1 Address Mapping Rules .....	25-12
Figure 25-21 Menu 15.3 Trigger Port Setup .....	25-12
Figure 26-1 Menu 21.2 Firewall Setup .....	26-1
Figure 27-1 Outgoing Packet Filtering Process .....	27-1
Figure 27-2 Filter Rule Process .....	27-2
Figure 27-4 Menu 21: Filter and Firewall Setup .....	27-3
Figure 27-5 Menu 21.1: Filter Set Configuration .....	27-3
Figure 27-6 Menu 21.1.1.1 TCP/IP Filter Rule .....	27-5
Figure 27-7 Executing an IP Filter .....	27-7
Figure 27-8 Menu 21.1.4.1 Generic Filter Rule .....	27-8
Figure 27-9 Telnet Filter Example .....	27-9
Figure 27-10 Example Filter: Menu 21.1.3.1 .....	27-10
Figure 27-11 Example Filter Rules Summary: Menu 21.1.3 .....	27-11
Figure 27-12 Protocol and Device Filter Sets .....	27-12
Figure 27-13 Filtering LAN Traffic .....	27-12
Figure 27-14 Filtering Remote Node Traffic .....	27-13
Figure 28-1 SNMP Management Model .....	28-1
Figure 28-2 Menu 22 SNMP Configuration .....	28-2
Figure 29-1 Menu 23 System Security .....	29-1
Figure 29-2 Menu 23 System Security .....	29-1
Figure 29-3 Menu 23.2 System Security : RADIUS Server .....	29-1
Figure 29-4 Menu 23 System Security .....	29-2
Figure 29-5 Menu 23.4 System Security : IEEE802.1x .....	29-3
Figure 30-1 Menu 24 System Maintenance .....	30-1
Figure 30-2 Menu 24.1 System Maintenance : Status .....	30-2
Figure 30-3 Menu 24.2 System Information and Console Port Speed .....	30-3
Figure 30-4 Menu 24.2.1 System Maintenance : Information .....	30-3
Figure 30-5 Menu 24.2.2 System Maintenance : Change Console Port Speed .....	30-4
Figure 30-6 Menu 24.3.2 System Maintenance : Syslog Logging .....	30-4
Figure 30-7 Call-Triggering Packet Example .....	30-6
Figure 30-8 Menu 24.4 System Maintenance : Diagnostic .....	30-7
Figure 30-9 LAN & WAN DHCP .....	30-7
Figure 31-1 Telnet in Menu 24.5 .....	31-2
Figure 31-2 FTP Session Example .....	31-2
Figure 31-3 Telnet into Menu 24.6 .....	31-5
Figure 31-4 Restore Using FTP Session Example .....	31-5
Figure 31-5 Telnet Into Menu 24.7.1 Upload System Firmware .....	31-6
Figure 31-6 Telnet Into Menu 24.7.2 System Maintenance .....	31-6
Figure 31-7 FTP Session Example of Firmware File Upload .....	31-7
Figure 32-1 Command Mode in Menu 24 .....	32-1

Figure 32-2 Valid Commands ..... 32-2

Figure 32-3 Menu 24.9 System Maintenance : Call Control ..... 32-2

Figure 32-4 Budget Management ..... 32-2

Figure 32-5 Call History..... 32-3

Figure 32-6 Menu 24: System Maintenance ..... 32-4

Figure 32-7 Menu 24.10 System Maintenance: Time and Date Setting ..... 32-4

Figure 33-1 Menu 24.11 – Remote Management Control ..... 33-1

Figure 34-1 Menu 26 Schedule Setup ..... 34-1

Figure 34-2 Menu 26.1 Schedule Set Setup ..... 34-2

Figure 34-3 Applying Schedule Set(s) to a Remote Node (PPPoE) ..... 34-3

# List of Tables

Table 1-1 IEEE 802.11b .....	1-2
Table 1-2 IEEE 802.11g .....	1-3
Table 2-1 Wizard Step 1 : Administrator Password .....	2-2
Table 2-2 Wizard Step 2 : Wireless LAN Setup .....	2-3
Table 2-3 Wizard Step 2 : Wireless LAN Setup Basic Security .....	2-4
Table 2-4 Wizard Step 2 : Wireless LAN Setup Extend Security .....	2-5
Table 2-5 Wizard Step 3 : Internet Access Setup .....	2-6
Table 2-6 Wizard Step 3 : ISP Parameters .....	2-6
Table 2-7 Wizard Step 3 : Internet Access Setup .....	2-7
Table 2-8 Wizard Step 3 : Internet Access Static IP Address Setup .....	2-8
Table 2-9 Wizard Step 4 : Parental Control Wizard .....	2-9
Table 2-10 Wizard Step 4 : Parental Control Time Setup .....	2-10
Table 2-11 Wizard Step 4 : Create or Edit a Profile .....	2-11
Table 2-12 Wizard Step 4 : Parental Control Profile Information .....	2-12
Table 2-13 Wizard Step 4 : Parental Control User Group .....	2-13
Table 2-14 Wizard Step 4 : Parental Control Time Allowance .....	2-14
Table 2-15 Wizard Step 4 : Parental Control Application Blocking .....	2-15
Table 2-16 Wizard Step 4 : Parental Control Summary .....	2-16
Table 2-17 Screens Summary .....	2-22
Table 3-1 Connection Wizard : Wireless LAN Setup .....	3-2
Table 3-2 Connection Wizard: Wireless LAN Setup: Basic Security .....	3-3
Table 3-3 Connection Wizard: Wireless LAN Setup: Extend Security .....	3-4
Table 3-4 Connection Wizard : Ethernet Encapsulation .....	3-5
Table 3-5 Connection Wizard : PPPoE Encapsulation .....	3-6
Table 3-6 Connection Wizard : PPTP Encapsulation .....	3-7
Table 3-7 Private IP Address Ranges .....	3-8
Table 3-8 Example of Network Properties for LAN Servers with Fixed IP Addresses .....	3-10
Table 3-9 Connection Wizard : WAN Setup .....	3-10
Table 4-1 SYSTEM : General Setup .....	4-1
Table 4-2 SYSTEM : DDNS .....	4-3
Table 4-3 SYSTEM : Password .....	4-4
Table 4-4 SYSTEM : Time Setting .....	4-5
Table 5-1 LAN : IP .....	5-4
Table 5-2 LAN : Static DHCP .....	5-7
Table 5-3 LAN : IP Alias .....	5-7
Table 6-1 WLAN : Wireless .....	6-5
Table 6-2 WLAN : Roaming .....	6-7
Table 7-1 WLAN : Wireless : No Security .....	7-2
Table 7-2 Wireless Security Relational Matrix .....	7-3
Table 7-3 WLAN : Wireless : Static WEP Encryption .....	7-5
Table 7-4 WLAN : Wireless : WPA-PSK .....	7-8
Table 7-5 WLAN : Wireless : WPA .....	7-11

Table 7-6 WLAN : Wireless : 802.1x and Dynamic WEP.....	7-13
Table 7-7 WLAN : Wireless : 802.1x and Static WEP .....	7-14
Table 7-8 WLAN : Wireless: 802.1x .....	7-16
Table 7-9 WLAN : MAC Address Filter .....	7-18
Table 7-10 WLAN : Local User Database.....	7-19
Table 7-11 WLAN : RADIUS .....	7-22
Table 8-1 WAN : Route .....	8-2
Table 8-2 WAN ISP : Ethernet Encapsulation .....	8-2
Table 8-3 WAN ISP : PPPoE Encapsulation.....	8-4
Table 8-4 WAN ISP : PPTP Encapsulation.....	8-5
Table 8-5 WAN : IP .....	8-6
Table 8-6 WAN : Traffic Redirect.....	8-10
Table 9-1 NAT Definitions .....	9-1
Table 9-2 NAT Mapping Types .....	9-4
Table 9-3 Services and Port Numbers .....	9-5
Table 9-4 SUA/NAT Setup .....	9-7
Table 9-5 Address Mapping.....	9-8
Table 9-6 Address Mapping Edit .....	9-9
Table 9-7 Trigger Port .....	9-11
Table 10-1 Static Route .....	10-2
Table 10-2 Static Route: Edit.....	10-2
Table 11-1 Configuring UPnP .....	11-2
Table 12-1 Parental Control.....	12-4
Table 12-2 Default Blocked Web categories.....	12-7
Table 12-3 Parental Control : Filter .....	12-8
Table 12-4 Services .....	12-14
Table 12-5 Parental Control : Edit.....	12-16
Table 12-6 Parental Control : Bypass List.....	12-18
Table 13-1 Firewall: Settings.....	13-2
Table 13-2 Firewall: Service.....	13-5
Table 14-1 Remote Management : WWW .....	14-2
Table 14-2 Remote Management : Telnet.....	14-4
Table 14-3 Remote Management : FTP.....	14-5
Table 14-4 SNMP Traps .....	14-7
Table 14-5 Remote Management : SNMP.....	14-8
Table 14-6 Remote Management : DNS.....	14-9
Table 14-7 Remote Management : Security .....	14-10
Table 15-1 View Logs.....	15-1
Table 15-2 Log Settings.....	15-3
Table 16-1 Maintenance : Status.....	16-1
Table 16-2 Maintenance : System Statistics .....	16-2
Table 16-3 Maintenance : DHCP Table .....	16-3
Table 16-4 Maintenance : Any IP .....	16-4
Table 16-5 Maintenance : Association List.....	16-4



Table 16-6 Maintenance : Firmware Upload .....	16-5
Table 16-7 Maintenance : Restore Configuration .....	16-7
Table 17-1 Main Menu Commands .....	17-2
Table 17-2 Main Menu Summary .....	17-3
Table 18-1 Menu 1 General Setup .....	18-1
Table 18-2 Menu 1.1 Configure Dynamic DNS .....	18-3
Table 19-1 Menu 2 WAN Setup .....	19-1
Table 20-1 Menu 3.2: DHCP Ethernet Setup Fields .....	20-2
Table 20-2 Menu 3.2: LAN TCP/IP Setup Fields .....	20-3
Table 20-3 Menu 3.2.1: IP Alias Setup .....	20-5
Table 20-4 Menu 3.5 Wireless LAN Setup .....	20-5
Table 20-5 Menu 3.5.1 WLAN MAC Address Filter .....	20-8
Table 20-6 Menu 3.5.2 Roaming Configuration .....	20-9
Table 21-1 Menu 4: Internet Access Setup (Ethernet) .....	21-1
Table 21-2 New Fields in Menu 4 (PPTP) Screen .....	21-3
Table 21-3 New Fields in Menu 4 (PPPoE) screen .....	21-3
Table 22-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation .....	22-2
Table 22-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific) .....	22-4
Table 22-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation .....	22-5
Table 22-4 Remote Node Network Layer Options .....	22-5
Table 22-5 Menu 11.6: Traffic Redirect Setup .....	22-8
Table 23-1 Menu 12.1 Edit IP Static Route .....	23-1
Table 24-1 Menu 14.1- Edit Dial-in User .....	24-1
Table 25-1 Applying NAT in Menus 4 & 11.3 .....	25-2
Table 25-2 SUA Address Mapping Rules .....	25-3
Table 25-3 Menu 15.1.1 First Set .....	25-5
Table 25-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	25-5
Table 25-5 Menu 15.3 Trigger Port Setup .....	25-13
Table 27-1 Abbreviations Used in the Filter Rules Summary Menu .....	27-3
Table 27-2 Rule Abbreviations Used .....	27-4
Table 27-3 TCP/IP Filter Rule .....	27-5
Table 27-4 Generic Filter Rule Menu Fields .....	27-8
Table 28-1 Menu 22 SNMP Configuration .....	28-2
Table 28-2 SNMP Traps .....	28-3
Table 28-3 Ports and Permanent Virtual Circuits .....	28-3
Table 29-1 Menu 23.2 System Security : RADIUS Server .....	29-2
Table 29-2 Menu 23.4 System Security : IEEE802.1x .....	29-3
Table 30-1 System Maintenance: Status Menu Fields .....	30-2
Table 30-2 Menu 24.2.1 System Maintenance : Information .....	30-3
Table 30-3 Menu 24.3.2 System Maintenance : Syslog and Accounting .....	30-4
Table 30-4 System Maintenance Menu Diagnostic .....	30-7
Table 31-1 Filename Conventions .....	31-1
Table 31-2 General Commands for GUI-based FTP Clients .....	31-3
Table 31-3 General Commands for GUI-based TFTP Clients .....	31-4

Table 32-1 Budget Management..... 32-3

Table 32-2 Call History Fields..... 32-3

Table 32-3 Time and Date Setting Fields ..... 32-4

Table 33-1 Menu 24.11 – Remote Management Control..... 33-1

Table 34-1 Menu 26.1 Schedule Set Setup ..... 34-2

---

# Preface

## About This User's Manual

Congratulations on your purchase of the HS-100 Parental Control Gateway or HS-100W Parental Control Gateway. This manual is designed to guide you through the configuration of your HomeSafe for its various applications.



**Some parts of this manual relate to the Wireless Parental Control Gateway.**

---



**Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your HomeSafe. Not all features can be configured through all interfaces.**

---

The web configurator parts of this guide contain background information on features configurable by the web configurator and the SMT. The SMT parts of this guide contain background information solely on features not configurable by the web configurator.

This manual may refer to the HS-100, HS-100W, Parental Control Gateway or Wireless Parental Control Gateway as the HomeSafe.

## Related Documentation

- **Support Disk**  
Refer to the included CD for support documents.
- **Quick Start Guide**  
The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- **Web Configurator Online Help**  
Embedded web help for descriptions of individual screens and supplementary information.
- **Packing List Card**  
The Packing List Card lists all items that should have come in the package.
- **Certifications**  
Refer to the product page at [www.zyxel.com](http://www.zyxel.com) for information on product certifications.
- **ZyXEL Glossary and Web Site**  
Please refer to [www.zyxel.com](http://www.zyxel.com) for an online glossary of networking terms and additional support documentation.













## User's Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

## Syntax Conventions

- The version number on the title page is the latest firmware version that is documented in this *User's Guide*. Earlier versions may also be included.
- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use “e.g.” as a shorthand for “for instance” and “i.e.” for “that is” or “in other words” throughout this manual.

## Graphics Icons Key

 HS-100W	 Computer	 Notebook computer
 Server	 Modem	 Firewall
 Telephone	 Switch	 Router
 DSLAM	 Wireless Access Point	 Wireless Signal



---

---

# Part I:

---

## Getting Started

---

This part helps you get to know your HomeSafe, introduces the web configurator and covers how to configure the Connection and Parental Control Wizard Setup screens.



# Chapter 1

## Getting to Know Your HomeSafe

*This chapter introduces the main features and applications of the HomeSafe.*

### 1.1 HomeSafe Parental Control Gateway Overview

HomeSafe is a parental control security gateway that can give a parent control over a child's Internet access privileges. It is the ideal secure gateway for all data passing between the Internet and LAN's.

By integrating web content filtering, NAT, firewall, ZyXEL's HomeSafe protects your Intranet and efficiently manages data traffic on your network.

The embedded web configurator is easy to operate.

### 1.2 HomeSafe Features

The following sections describe HomeSafe features.

#### 1.2.1 Physical Features

##### **10/100M Auto-negotiating Ethernet/Fast Ethernet Interface(s)**

This auto-negotiation feature allows the HomeSafe to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

##### **Auto-crossover 10/100 Mbps Ethernet Interface(s)**

These interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

##### **4-Port Switch**

A combination of switch and router makes your HomeSafe a cost-effective and viable network solution. You can add up to four computers to the HomeSafe without the cost of a hub. Add more than four computers to your LAN by using a hub.

##### **Time and Date**

The HomeSafe allows you to get the current time and date from an external server when you turn on your HomeSafe. You can also set the time manually.

##### **Reset Button**

The HomeSafe reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

#### 1.2.2 Non-Physical Features

##### **Parental Control**

The HomeSafe can control access privileges to website and services through Parental Control. Parental Control can be defined as the ability for a parent (LAN administrator) to control a child's (LAN user) Internet access privileges. The administrator can create a login name and password for each user on the network. Up to ten user accounts can be configured. Each user must log into the system before they can gain access to the Internet. Each account will have specific access restrictions.



## Content Filtering

The HomeSafe can block access to Internet services according to how you configure parental control application blocking. You can define time periods and days during which content filtering is enabled and include or exclude categories on the LAN.

## Firewall

The HomeSafe is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The HomeSafe firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

### IEEE 802.1x Network Security (HS-100W only)

The HomeSafe supports the IEEE 802.1x standard to enhance user authentication. Use the built-in user profile database to authenticate up to 32 users using MD5 encryption. Use an EAP-compatible RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate users using EAP (Extensible Authentication Protocol). EAP is an authentication protocol that supports multiple types of authentication.

### Brute-Force Password Guessing Protection

The HomeSafe has a special protection mechanism to discourage brute-force password guessing attacks on the HomeSafe's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.

### 802.11b Wireless LAN Standard (HS-100W only)

The HomeSafe, complies with the IEEE 802.11b wireless standard.

The IEEE 802.11b data rate and corresponding modulation techniques are as follows. The modulation technique defines how bits are encoded onto radio waves.

**Table 1-1 IEEE 802.11b**

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)



**The HomeSafe may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.**

### 802.11g Wireless LAN Standard (HS-100W only)

The HomeSafe, complies with the IEEE 802.11g wireless standard and is also fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b wireless card can interface directly with an IEEE 802.11g device (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 1-2 IEEE 802.11g**

<b>DATA RATE (MBPS)</b>	<b>MODULATION</b>
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

**Packet Filtering**

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

**Universal Plug and Play (UPnP)**

Using the standard TCP/IP protocol, the HomeSafe and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

**Call Scheduling**

Configure call time periods to restrict and allow access for users on remote nodes.

**PPPoE**

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

**PPTP Encapsulation**

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The HomeSafe supports one PPTP server connection at any given time.

**Dynamic DNS Support**

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

**IP Multicast**

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the HomeSafe supports both versions 1 and 2.

**IP Alias**

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The HomeSafe supports three logical LAN interfaces via its single physical Ethernet LAN interface with the HomeSafe itself as the gateway for each LAN network.

**SNMP**

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your HomeSafe supports SNMP agent functionality, which allows a manager station to manage and monitor the HomeSafe through the network. The HomeSafe supports SNMP version one (SNMPv1).

## **Network Address Translation (NAT)**

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

### **Traffic Redirect**

Traffic Redirect forwards WAN traffic to a backup gateway on the LAN when the HomeSafe cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

### **Port Forwarding**

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

### **DHCP (Dynamic Host Configuration Protocol)**

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The HomeSafe has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The HomeSafe can also act as a surrogate DHCP server where it relays IP address assignments from the actual DHCP server to the clients.

### **Any IP**

The Any IP feature allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the HomeSafe are not in the same subnet.

### **Full Network Management**

The embedded web configurator is an all-platform web-based utility that allows you to easily access the HomeSafe's management settings and configure the firewall. Most functions of the HomeSafe are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access over a telnet connection.

### **RoadRunner Support**

In addition to standard cable modem services, the HomeSafe supports Time Warner's RoadRunner Service.

### **Logging and Tracing**

- Built-in message logging and packet tracing.
- Unix syslog facility support.
- Firewall logs.
- Content filtering logs.

### **Upgrade HomeSafe Firmware via LAN**

The firmware of the HomeSafe can be upgraded via the LAN (*refer to Maintenance- F/W Upload Screen*).

### **Embedded FTP and TFTP Servers**

The HomeSafe's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

### Wireless Association List (HS-100W only)

With the wireless association list, you can see the list of the wireless stations that are currently using the HomeSafe to access your wired network.

## 1.3 Applications for the HomeSafe

Here are some examples of HomeSafe applications.

### 1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

You can connect a cable modem, DSL or wireless modem to the HomeSafe for broadband Internet access via an Ethernet or a wireless port on the modem. The HomeSafe guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

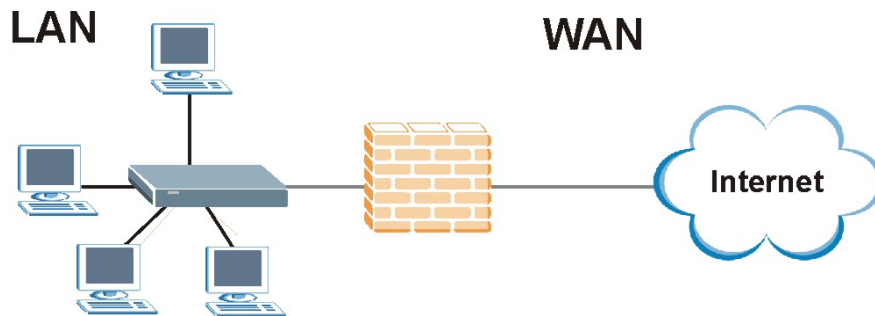


Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem

### 1.3.2 HomeSafe Parental Control Gateway

You can control LAN user Internet access by having an administrator configure parental control on the HomeSafe.

The parent (administrator) must create login names and passwords for each person (user) on the network. Each person must log into the system before they can gain access to the Internet. Each person's account will hold the details of their access rights and privileges. The HomeSafe enforces these access restrictions. In the following diagram, A refers to the HomeSafe and B refers to a modem.

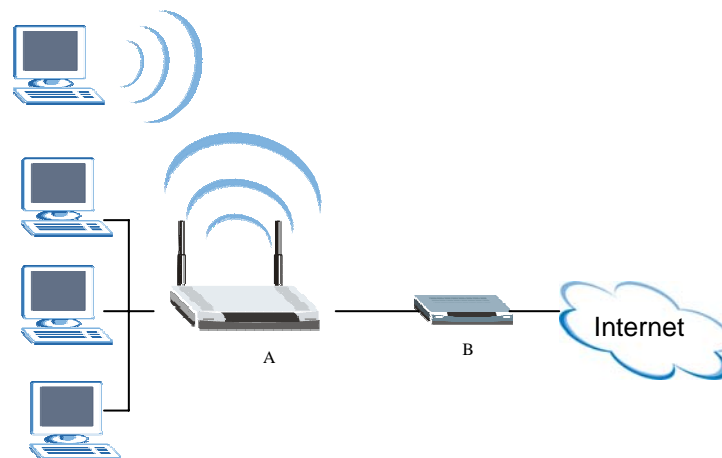
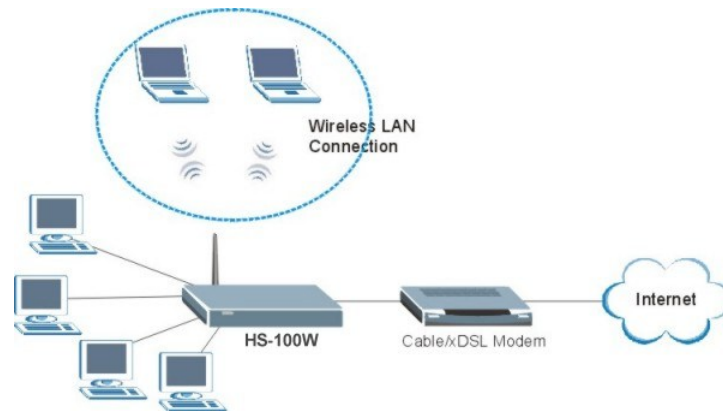


Figure 1-2 HomeSafe Parental Control Gateway Application

### 1.3.3 Wireless LAN Application

Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.



**Figure 1-3 Wireless LAN Application Example**

## Chapter 2

# Introducing the Web Configurator

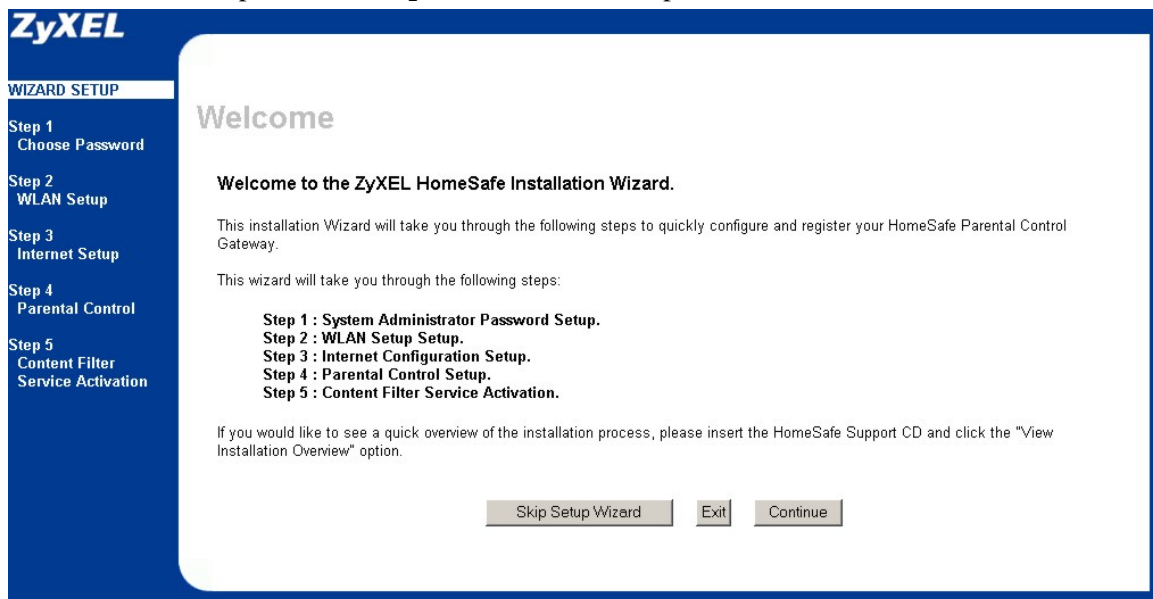
*This chapter describes how to access the HomeSafe web configurator and provides an overview of the initial configuration screens.*

### 2.1 Web Configurator Overview

The embedded web configurator allows you to manage the HomeSafe from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual HomeSafe models or firmware versions.

### 2.2 Accessing the HomeSafe Web Configurator

1. Make sure your HomeSafe hardware is properly connected and prepare your computer/computer network to connect to the HomeSafe (refer to the *Quick Start Guide*).
2. Launch your web browser.
3. Enter "192.168.1.1" as the URL.
4. The HomeSafe **Welcome** screen appears. Read the on screen information and click **Continue** to proceed to **Step 1** of the wizard setup.



**Figure 2-1 Welcome Menu**

- Click **Exit** to close your web browser.
- Click **Skip Setup Wizard** to proceed to the **MAIN MENU** screen without using the configuration wizard. See the section Accessing the HomeSafe Web Configurator for instructions on configuring your device without using the wizard.



The Welcome screen only appears when you first enter the HomeSafe web browser. After you fully configure the wizard you automatically proceed to the Password screen for all future logins, see *Figure 2-25*. You may go to the Welcome screen after initial configuration, only by resetting your HomeSafe to factory defaults.

---

## 2.3 Step 1 : System Administrator Password Setup

You can configure your system password in the following screen.

**System Administrator Password**

Please select a unique System Administrator's password (up to 30 characters long).

You will need this password whenever you want to access the system management interface to change any of the system settings.

You should select a password that you can easily remember or write it down and keep it in a safe place as you will not be able to gain access to the system management interface in the future without it.

**Password**

**Confirm Password**

**Figure 2-2 Wizard Step 1 : Administrator Password**

The following table describes the fields in this screen.

**Table 2-1 Wizard Step 1 : Administrator Password**

LABEL	DESCRIPTION
Password	Type a password. After initial configuration, this password is used each time you log into the web configurator, see <i>Figure 2-25</i> .
Confirm Password	Retype the password to confirm.
Back	Click <b>Back</b> to display the previous screen.
Continue	Click <b>Continue</b> to proceed to the next screen.

## 2.4 Step 2 : WLAN Setup

Set up your wireless LAN using the second wizard screen.

**Wireless LAN Setup**

☒ **Enable Wireless LAN**

**ESSID Configuration**

Enter a unique name for your wireless network (ESSID). You will need to remember this name for connecting to your wireless network.

ESSID

**Channel Selection**

Select which channel you want your wireless network to operate on.

Channel

**Security Configuration**

Choose what level of security you would like to use on your wireless network.

- No Security : Anyone can connect to your home network
- Basic Security : Provides basic encryption and access control (WEP)
- Extend Security : High level encryption and basic access control (WPA-PSK)

Security

**Figure 2-3 Wizard Step 2 : Wireless LAN Setup**

The following table describes the fields in this screen.

**Table 2-2 Wizard Step 2 : Wireless LAN Setup**

LABEL	DESCRIPTION
ESSID	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the HomeSafe, make sure all wireless stations use the same ESSID in order to access the network.
Choose Channel ID	To set the HomeSafe to use a channel, select a channel from the drop-down list box.
Security	The level of <b>Security</b> can be selected as none, basic or extended. Choose <b>No</b> security to have no wireless LAN security configured and proceed to the <b>ISP Parameters for Internet Access</b> screen. Choose <b>Basic</b> security if you want to configure <b>WEP Encryption</b> parameters. Choose <b>Extend</b> security to configure a <b>Pre-Shared Key</b> . The following screen varies depending on which security level you select.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.4.1 Step 2 : WLAN Setup Basic Security

If you choose **Basic**, you can setup WEP Encryption parameters.



**The wireless stations and HomeSafe must use the same ESSID, channel ID and WEP encryption key for wireless communication.**



**Wireless LAN Setup**

**WEP Encryption**

Select your level of encryption. 128-bit provides better encryption but slightly slower performance.

64-bit WEP

Enter in your WEP keys. These are similar to passwords that will be used to restrict access to your wireless network. Each wireless user will need to know them in order to connect. If you have chosen 64-bit encryption the keys should be 5 characters in length. If you chose 128-bit encryption each key should be 13 characters in length.

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).  
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).  
(Select one WEP key as an active key to encrypt wireless data transmission.)

☒ ASCII (Plain Text) ☐ Hex

☒ Key 1

☐ Key 2

☐ Key 3

☐ Key 4

Back Next

Figure 2-4 Wizard Step 2 : Wireless LAN Setup Basic Security

The following table describes the labels in this screen.

Table 2-3 Wizard Step 2 : Wireless LAN Setup Basic Security

LABEL	DESCRIPTION
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the HomeSafe and the wireless stations must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.4.2 Step 2 : WLAN Setup Extended Security

If you choose **Extend** security in the Wireless LAN Setup screen, you can set up a Pre-Shared Key.



**The wireless stations and HomeSafe must use the same ESSID, channel ID and Pre-Shared Key for wireless communication.**

**Figure 2-5 Wizard Step 2 : Wireless LAN Setup Extend Security**

The following table describes the labels in this screen.

**Table 2-4 Wizard Step 2 : Wireless LAN Setup Extend Security**

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

Refer to the chapter on wireless LAN for more information.

## 2.5 Step 3 : Internet Configuration Setup

By implementing PPPoE directly on the HomeSafe (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the HomeSafe does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

**Figure 2-6 Wizard Step 3 : Internet Access Setup**

The following table describes the labels in this screen.

**Table 2-5 Wizard Step 3 : Internet Access Setup**

LABEL	DESCRIPTION
Are you using a DSL service provider that requires a PPPoE login name and password?	Select <b>Yes</b> from the drop-down list box if you are using a DSL service provider that requires PPPoE login information.  Select <b>No</b> from the drop-down list box if your service provider does not require you to enter PPPoE information. You can select whether to configure a static WAN IP address or have it assigned dynamically.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.5.1 Step 3 : Internet Configuration Setup ISP Parameters

If you click **Yes** in the previous screen, you must type your PPPoE login name and password.

The screenshot shows a web interface titled "Internet Configuration Setup". Inside, there's a yellow rectangular area with the heading "ISP Parameters for Internet Access". Below this, it says "Enter your PPPoE login name and password." followed by two input fields labeled "User Name" and "Password". At the bottom right of the yellow area are two buttons: "Back" and "Next".

**Figure 2-7 Wizard Step 3 : ISP Parameters**

The following table describes the labels in this screen.

**Table 2-6 Wizard Step 3 : ISP Parameters**

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the Figure 2-10 screen.

### 2.5.2 Step 3 : Internet Access Setup

If you click **No** in the **Internet Access Setup** screen you must select **DHCP** or **Static** WAN IP address assignment.

**Internet Configuration Setup**

**Internet Access Setup**

Is your Internet connection configured for DHCP or Static IP address assignment? If you are not sure, you should select DHCP as it is by far the most common.

☒ **DHCP**  
☐ **Static**

Back Next

**Figure 2-8 Wizard Step 3 : Internet Access Setup**

The following table describes the labels in this screen.

**Table 2-7 Wizard Step 3 : Internet Access Setup**

LABEL	DESCRIPTION
DHCP	Select <b>DHCP</b> to have your Internet connection configured for dynamic WAN IP address assignment.
Static	Select <b>Static</b> to manually setup your WAN IP address.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to <i>Figure 2-10</i> if you select <b>DHCP</b> in this screen or proceed to the following screen if you select <b>Static</b> .

### 2.5.3 Step 3 : Internet Access Static IP Address Setup

If you select **Static** in the previous screen you must configure your WAN IP address and DNS server address(es).

**Internet Configuration Setup**

**Internet Access Setup**

My WAN IP Address 0.0.0.0

My WAN IP Subnet Mask 0.0.0.0

Gateway IP Address 0.0.0.0

**DNS Server Address Assignment**

First DNS Server From ISP 0.0.0.0

Second DNS Server From ISP 0.0.0.0

Third DNS Server From ISP 0.0.0.0

Back Next

**Figure 2-9 Wizard Step 3 : Internet Access Static IP Address Setup**

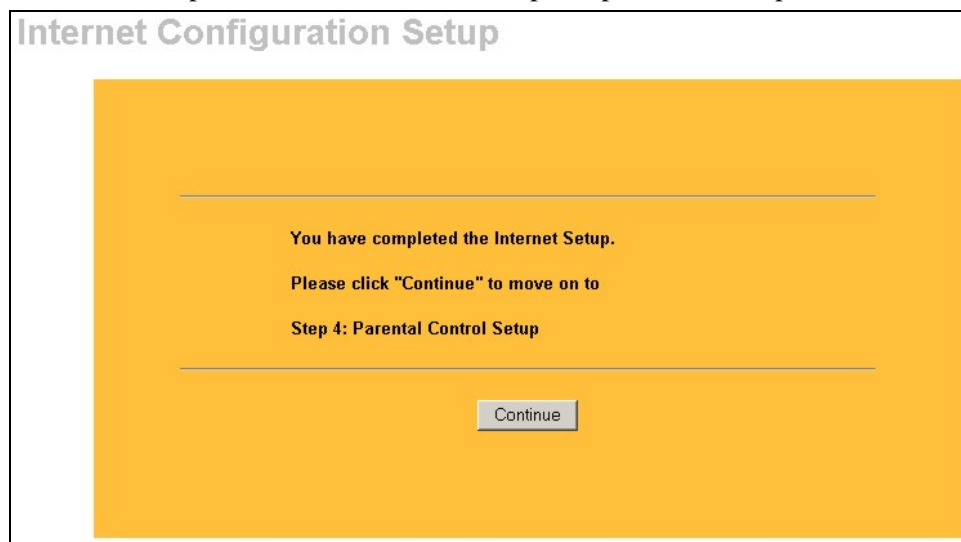
The following table describes the labels in this screen.

**Table 2-8 Wizard Step 3 : Internet Access Static IP Address Setup**

LABEL	DESCRIPTION
Internet Access Setup	
My WAN IP Address	Enter your WAN IP address in this field.
My WAN IP Subnet Mask	Type your network's IP subnet Mask.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field.
DNS Server Address Assignment (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The HomeSafe uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the HomeSafe's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.  Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.  Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Second DNS Server	
Third DNS Server	
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

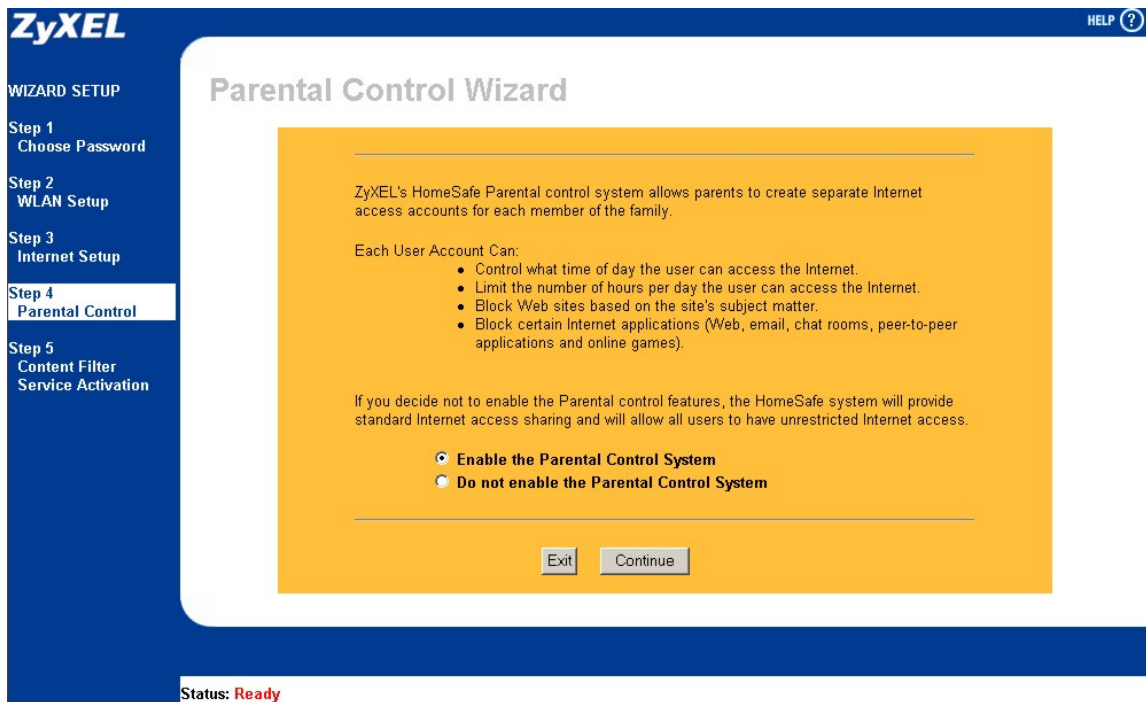
### 2.5.4 Step 3 : Internet Configuration Setup Complete

Click **Continue** to complete the wizard Internet setup and proceed to the parental control wizard.

**Figure 2-10 Wizard Step 3 : Internet Setup Complete**

## 2.6 Step 4 : Parental Control Wizard

The main parental control screen allows you to restrict or not restrict access to the Internet.



**Figure 2-11 Wizard Step 4 : Parental Control Wizard**

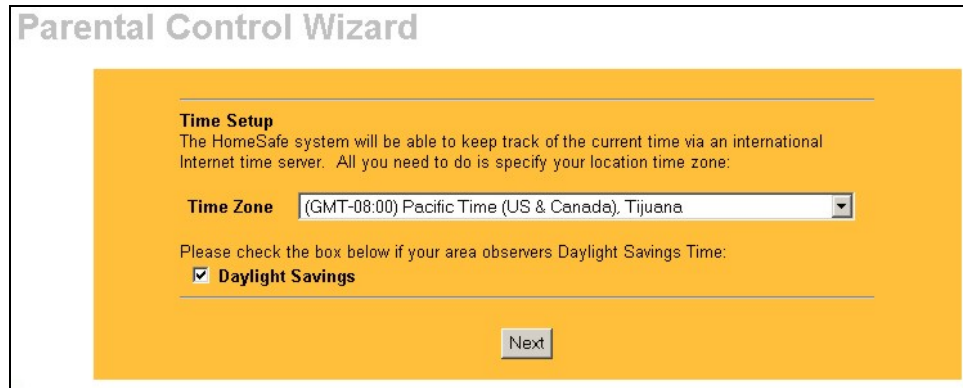
The following table describes the labels in this screen.

**Table 2-9 Wizard Step 4 : Parental Control Wizard**

LABEL	DESCRIPTION
Enable the Parental Control System	Select the check box to allow the parent (LAN administrator) to have access control over a child's (LAN user) Internet access.
Do not enable the Parental Control System	Select the check box to have no parental control configured.
Exit	Click <b>Exit</b> to stop configuring the wizard and close the web browser.
Continue	Click <b>Continue</b> to proceed to the next screen.

### 2.6.1 Step 4 : Parental Control Time Setup

Use this screen to configure the HomeSafe's time based on your local time zone.



**Figure 2-12 Wizard Step 4 : Parental Control Time Setup**

The following table describes the labels in this screen.

**Table 2-10 Wizard Step 4 : Parental Control Time Setup**

LABEL	DESCRIPTION
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.6.2 Step 4 : Parental Control Create or Edit a Profile

With Parental Control you can configure up to ten user profiles. View these profiles in this screen.

**Parental Control Wizard**

---

**Create/Edit a Profile**  
 The HomeSafe system requires that users login before they are allowed to access the Internet. Users will not be allowed to access the Internet unless they have a valid user name and password.

Each family member account must have a unique name.

User names and passwords are case sensitive and may be to up 30 characters long.

Create a new user account by selecting one of the empty accounts below and click next.

You may edit an existing account by selecting it from the list below and clicking next.

	Username	Group
<input checked="" type="radio"/>	Typhus	Mature Teen
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		
<input type="radio"/>		

**Figure 2-13 Wizard Step 4 : Create or Edit a Profile**

The following table describes the labels in this screen.

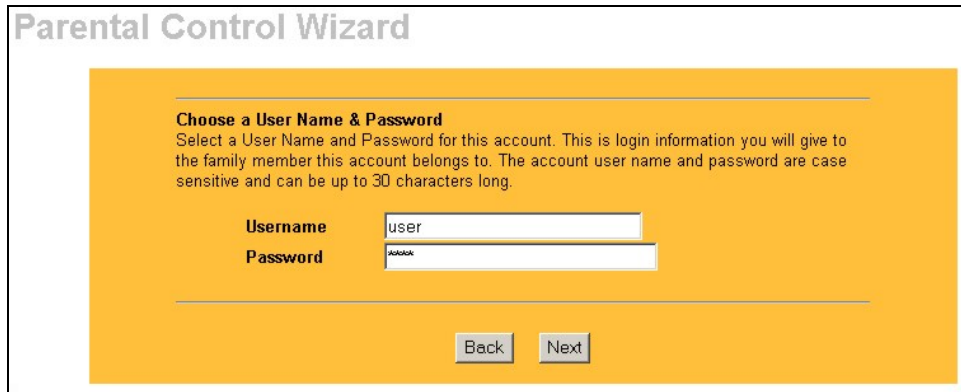
**Table 2-11 Wizard Step 4 : Create or Edit a Profile**

LABEL	DESCRIPTION
	Click a radio button to select a users profile.
Username	This field displays the username (up to 30 characters) for this user profile.
Group	This field displays the category of the profile user. <ul style="list-style-type: none"> <li>➤ Kids</li> <li>➤ Young Teen</li> <li>➤ Mature Teen</li> <li>➤ Adult</li> </ul> These groups are used in conjunction with content filtering to decide which web pages the user cannot access.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.6.3 Step 4 : Parental Control Profile Information

The parent (administrator) must create log in names and passwords for each person (user) on the network. Each user must log into the system before they can gain Internet access.





**Figure 2-14 Wizard Step 4 : Parental Control Profile Information**

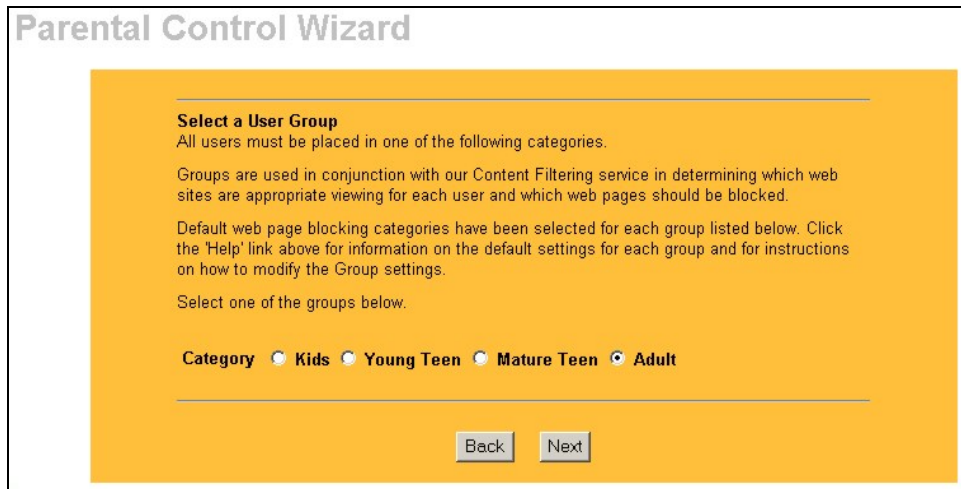
The following table describes the labels in this screen.

**Table 2-12 Wizard Step 4 : Parental Control Profile Information**

LABEL	DESCRIPTION
User Name	Type the profile user name.
Password	Type the password associated with the user name above.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

#### 2.6.4 Step 4 : Parental Control User Group


Choose a user group from the category shown in this screen. The configuration screens that follow are based on the user group that you select in this screen.



**Figure 2-15 Wizard Step 4 : Parental Control User Group**

The following table describes the labels in this screen.

Table 2-13 Wizard Step 4 : Parental Control User Group

Category	<p>Select a radio button to configure a user for one of the following categories:</p> <ul style="list-style-type: none"> <li>➤ Kids</li> <li>➤ Young Teen</li> <li>➤ Mature Teen</li> <li>➤ Adult</li> </ul> <hr/> <p> <b>The administrator can decide each group's access rights.</b></p> <hr/> <p>For example, if you do not want a child to access a chat room or instant messenger, you can select the category as <b>Kids</b> or <b>Young Teen</b> and block those services, see <i>Figure 2-17</i>. For information on default user categories, see the <i>Parental Control</i> chapter.</p>
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.6.5 Step 4 : Parental Control Time Allowance

This screen allows you to set the amount of time during each day a user can access the Internet. By default a new user account does not have permission to access the Internet.

**Parental Control Wizard**

---

**Daily Time and Allowance**  
The following settings will determine when this user may access the internet and for how long each day of the week.

Unrestricted  
Check the Unrestricted box to give this user unlimited time on the Internet for that day of the week.

Time Allowance  
Use the Time Allowance setting to limit the amount of time the user can spend logged onto the Internet. The user will be automatically logged off the Internet when their time allowance runs out.




Start/End Time  
Use these setting to set what time of day this user is allow to log into the Internet. This user will only be allowed on the Internet between these hours.

	Unrestricted	Time Allowance	Start Time	End Time
<b>Monday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾
<b>Tuesday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾
<b>Wednesday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾
<b>Thursday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾
<b>Friday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾
<b>Saturday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾
<b>Sunday</b>	<input type="checkbox"/>	0 hr 0 min	Midnight ▾	Midnight ▾

Figure 2-16 Wizard Step 4 : Parental Control Time Allowance

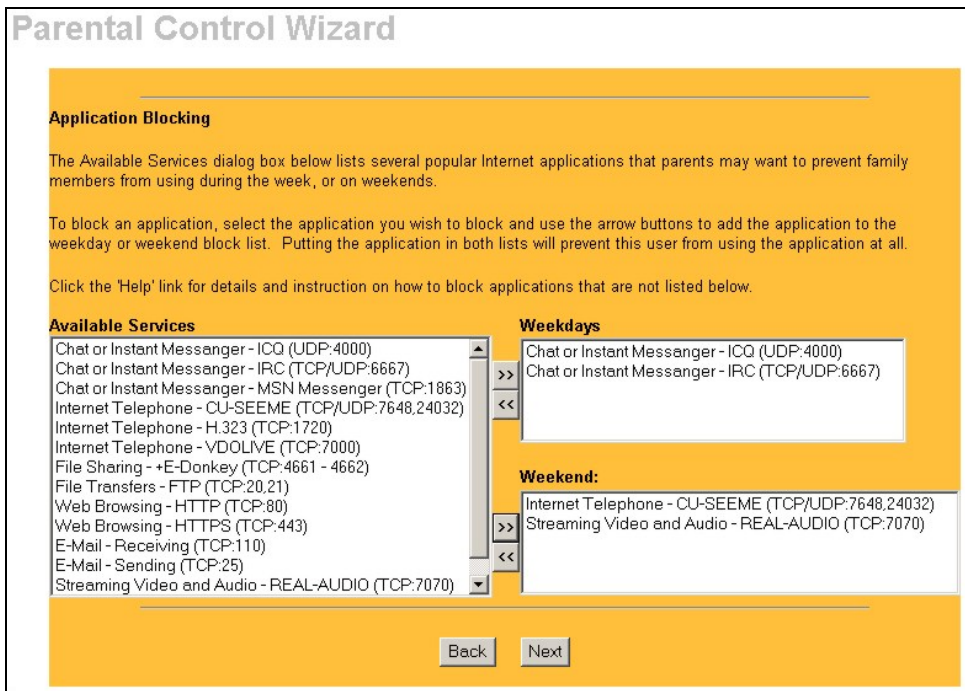
The following table describes the labels in this screen.

**Table 2-14 Wizard Step 4 : Parental Control Time Allowance**

LABEL	DESCRIPTION
Unrestricted	Select the check box for the day(s) that you do not want any time restrictions for user Internet access.   <b>If services have been blocked and the amount of time has been selected as unrestricted, a user will still be unable to access those services.</b>
Time Allowance (hr:min)	Type the number of hours (0 to 23) and minutes (0 to 59) to allow Internet access of unblocked sites.   <b>If you want to allow twenty-four hour access, you should select the unrestricted check box.</b>
Start Time	Select from the drop-down list box a time during the day when a user can begin accessing unblocked sites.
End Time	Select from the drop-down list box a time during the day when a user can no longer access unblocked sites. The time allowance must be less than or equal to the period from the start time to the end time.   <b>User access will be denied after the End Time for that day even if the time allowance has not run out.</b>
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.6.6 Step 4 : Parental Control Application Blocking

You can block services in the **Application Blocking Screen** for the user group.



**Figure 2-17 Wizard Step 4 : Parental Control Application Blocking**

The following table describes the labels in this screen.

**Table 2-15 Wizard Step 4 : Parental Control Application Blocking**

LABEL	DESCRIPTION
Available services	Select a service from the list and click the >> button to have the service blocked on a weekday (Monday to Friday), on a day in the weekend (Saturday or Sunday) or both. These services will be blocked according to the settings you configure in the <b>Daily Time and Allowance</b> screen.
Weekdays	This box shows all the services that you want to block on weekdays for the user group. Click the << button to remove a service from the box.
Weekend	This box shows all the services that you want to block on weekends for the user group. Click the << button to remove a service from the box.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

### 2.6.7 Step 4 : Parental Control Account Summary

The **Account Summary** screen displays a summary of information about a user account. From this screen you may proceed to add a new user account or edit an existing user account.

### Content Filter Service Activation

---

**Account Summary**

This page displays a summary of this user's account information.

Click the 'Back' button to change any of these settings.

Click the 'Add/Edit Another User' button to create or change another user account.

Click the 'Finish' button if you are finished creating or changing user accounts.

Username: user  
 Password:                       
 Group: Adult

**Time Management:**

	Unrestricted	Time Allowance	Start Time	End Time
Monday	No	0 hr 0 min	Midnight	Midnight
Tuesday	No	0 hr 0 min	Midnight	Midnight
Wednesday	No	0 hr 0 min	Midnight	Midnight
Thursday	No	0 hr 0 min	Midnight	Midnight
Friday	No	0 hr 0 min	Midnight	Midnight
Saturday	No	0 hr 0 min	Midnight	Midnight
Sunday	No	0 hr 0 min	Midnight	Midnight

**Service Blocking**

**Weekdays:**

Chat or Instant Messenger - IRC (TCP/UDP:6667)
Chat or Instant Messenger - ICQ (UDP:4000)

**Weekend:**

Internet Telephone - CU-SEEME (TCP/UDP:7648,24032)
Streaming Video and Audio - REAL-AUDIO (TCP:7070)

Back
Add/Edit Another User
Finish

**Figure 2-18 Wizard Step 4 : Parental Control Summary**

The following table describes the labels in this screen.

**Table 2-16 Wizard Step 4 : Parental Control Summary**

LABEL	DESCRIPTION
Back	Click <b>Back</b> to display the previous screen.
Add/Edit Another User	Click this button to proceed to the <b>Create/Edit a Profile</b> screen, see <i>Figure 2-13</i> . You can edit an existing account or add a new profile.
Finish	Click <b>Finish</b> to proceed to the next screen.

When you click **Finish**, the final Parental Control wizard screen appears.

### 2.6.8 Step 4 : Parental Control Register for Content Filter

The Content Filtering Service Status read only field displays **Not Registered** if you have not successfully registered the HomeSafe or your registration has expired.

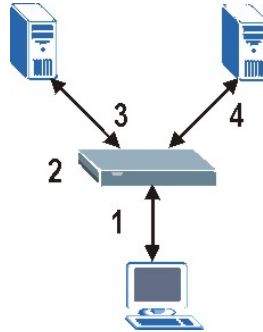
This field only displays whether or not you have successfully registered, not whether or not content filtering is active. See *Checking Content Filtering Activation* for details on how to check for this. Click **Register Now** to go to a web site where you can register for category-based content filtering (using an external database). You can use a trial application or register your iCard's PIN. Refer to the web site's on-line help for details.



**The web site displays a registration successful web page. It may take up to another ten minutes for content filtering to be activated. See *Checking Content Filtering Activation* for how to know if the content filtering has been activated.**

### Content Filtering with an External Server

Your HomeSafe uses a content filter lookup process as described below.



**Figure 2-19 Content Filtering Lookup Procedure**

1. A computer sends an HTTP request to a web server.
2. The HomeSafe looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the HomeSafe's cache. The HomeSafe either blocks or forwards the request based on how you configure the category based content filtering.

The HomeSafe drops a URL record from the content filter cache after the content filter cache timeout period (default 72 hours). All of the URL records are also cleared from the local cache when the HomeSafe reboots. You can use `ip urlfilter webControl cache timeout` on the command line to change the timeout period.

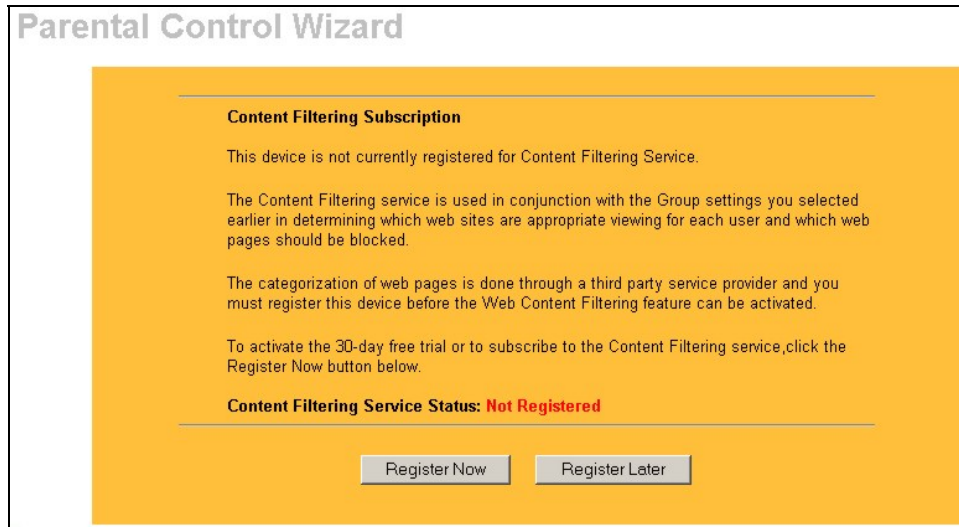
If the HomeSafe doesn't have a record of the web site, it will query the external content filtering server and simultaneously send the request to the web server.

The external content filtering database may change a web site's category or rate a previously uncategorized web site.

3. The external content filtering server sends the category information back to the HomeSafe, which then either forwards or blocks the web content. The web site address is then also stored in the HomeSafe's content filtering cache.

### Checking Content Filtering Activation

Since there will be no activation notice, when content filtering is active, you should see an access blocked message when your HomeSafe has been setup with parental control and you try to access a restricted website or service.



**Figure 2-20 Wizard Step 4 : Content Filter Registration**

If you click **Register Later** you will proceed to *Figure 2-24*.

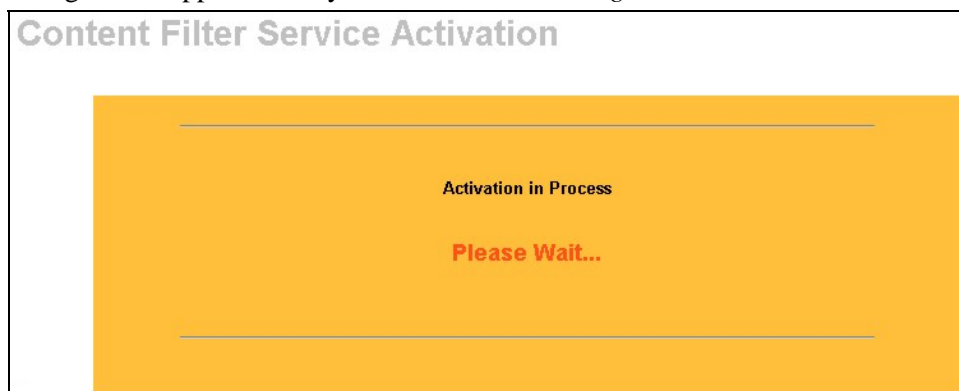
## 2.7 Step 5 : Content Filter Service Activation

Once you have completed the registration process you can click **Activate** to begin the content filtering service now or click **Activate Later** to activate the service at a later date.



**Figure 2-21 Content Filter Activation in Progress**

The following screen appears after you click **Activate** in *Figure 2-21*.



**Figure 2-22 Content Filter Activation in Progress**

If this is successful, you have completed the content filtering service activation.

Your device must be registered for content filtering service to activate successfully. If the activation fails, see the following screen and read the instructions.



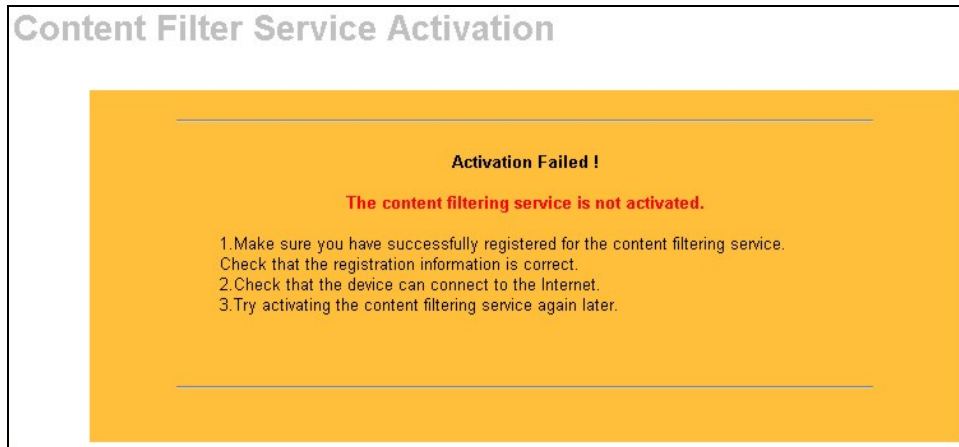


Figure 2-23 Content Filter Activation Failure

### 2.7.1 Content Filter Setup Complete

Well done! You have finished configuration of Content Filter Service Activation. You may now click **Close** to finish using the setup wizard and close your browser.

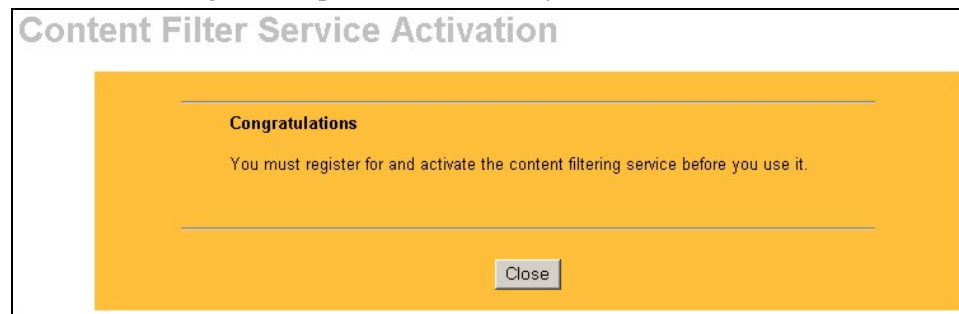


Figure 2-24 Content Filter Setup Complete



**To use the HomeSafe content filtering you must enable and configure Pre-defined Web Content Categories in the ADVANCED Parental Control group edit configuration screen.**

## 2.8 Accessing the Internet via the HomeSafe Gateway

If you are satisfied with the initial setup, you can access the Internet by following the steps below. You must first log into the HomeSafe to allow your computer on the network to gain Internet access.

1. When you open your browser, you are directed to the HomeSafe's User Login page.
2. By entering your login name and password the device checks the access profile and begins enforcing the access control restriction as defined by the administrator.
3. The access privileges remain in force until you log out.
4. After a successful login, the system displays a window that will display the budget time remaining, a logout button, and a link to open a new browser window to begin Internet surfing.
5. When done using the Internet, or to log-in another user, click the logout button or type **logout** in your web browsers address bar.



If you want to configure more of your HomeSafe features, proceed with the rest of this User's Guide.

## 2.9 Accessing the HomeSafe Web Configurator



**You have to open a new browser and enter the device IP address to log in again.**

1. Launch your web browser.
2. Type "192.168.1.1" as the URL.
3. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.



The image shows a web interface with a blue background. At the top, it says "HS-100/HS-100W". Below that, it says "Enter Password and click Login." There is a label "Password:" followed by a text input field containing "1234". At the bottom, there are two buttons: "Login" and "Reset".

**Figure 2-25 Password Screen**

4. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**. Refer to *Figure 2-14* if you have already configured your user password.



The image shows a web interface with a blue background. At the top, it says "Use this screen to change the password." Below that, there are two labels: "New Password:" and "Retype to Confirm:". Each label is followed by a text input field. The "New Password:" field contains "1234". At the bottom, there are two buttons: "Apply" and "Ignore".

**Figure 2-26 Change Password Screen**

5. You should now see the **MAIN MENU** screen (see *Figure 2-27*).



**The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the HomeSafe if this happens to you.**

## 2.10 Resetting the HomeSafe

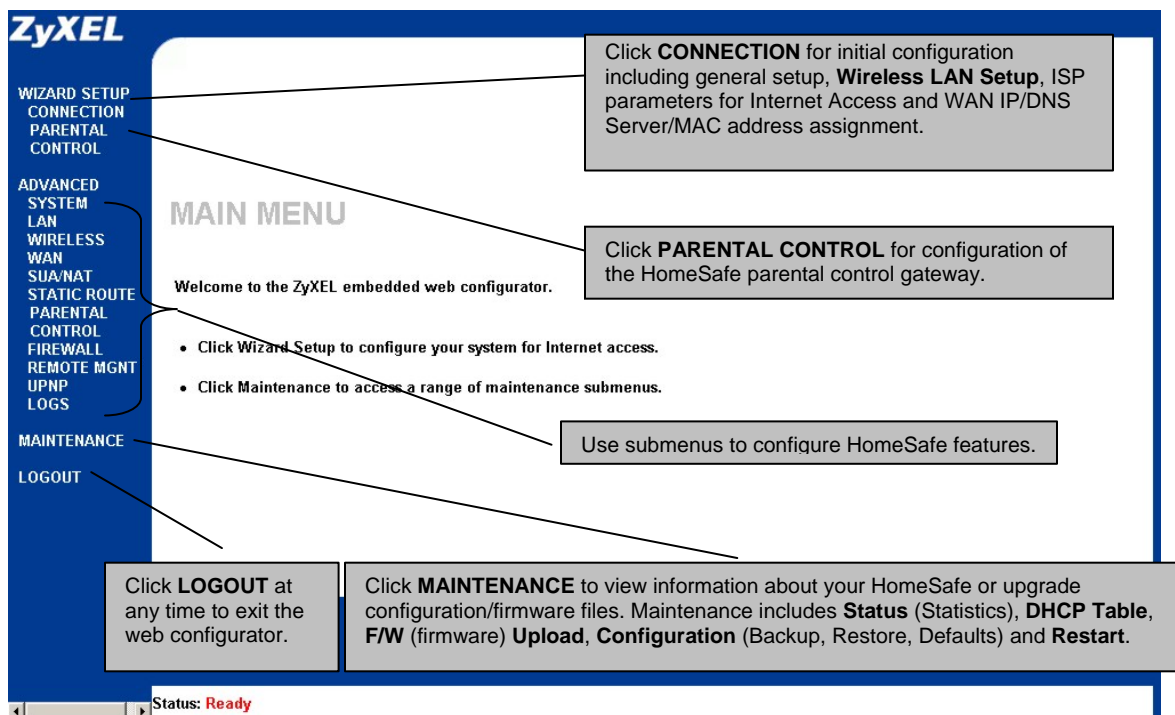
If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the HomeSafe to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

### 2.10.1 Procedure To Use The Reset Button

Make sure the **PWR** LED is on (not blinking) before you begin this procedure.

1. Make sure the **PWR** LED is on (not blinking).
2. Press the **RESET** button for ten seconds or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the HomeSafe restarts.

## 2.11 HomeSafe Main Menu



**Figure 2-27 The MAIN MENU Screen of the Web Configurator**

### 2.11.1 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure HomeSafe features.

The following table describes the sub-menus.

**Table 2-17 Screens Summary**

LINK	TAB	FUNCTION
WIZARD SETUP		
CONNECTION		Use these screens for initial configuration including general setup, Wireless LAN setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
PARENTAL CONTROL		Use these screens to create user profiles, configure a user category for blocking services, register for content filtering and configure time allowances.
ADVANCED		
SYSTEM	General	This screen contains administrative and system-related information.
	DDNS	Use this screen to set up dynamic DNS.
	Password	Use this screen to change your password.
	Time Zone	Use this screen to change your HomeSafe's time and date.
LAN	IP	Use this screen to configure LAN DHCP, TCP/IP settings and to enable Any IP.
	Static DHCP	Use this screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
	IP Alias	Use this screen to partition your LAN interface into subnets.
WIRELESS	Wireless	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the HomeSafe to block access to devices or block the devices from accessing the HomeSafe.
	Roaming	This screen allows you to configure your HomeSafe roaming capabilities.
	802.1x/WPA	This screen allows you to configure 802.1x enhanced security method for both the authentication of wireless stations and encryption key management.
	Local User Database	This screen allows you to configure a database internal to the HomeSafe.
	RADIUS	This screen allows you to configure an external RADIUS server for an unlimited number of users.
WAN	Route	This screen allows you to configure route priority.
	WAN ISP	Use this screen to change your HomeSafe's WAN ISP settings.
	WAN IP	Use this screen to change your HomeSafe's WAN IP address settings.
	WAN MAC	Use this screen to change your HomeSafe's WAN MAC settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
SUA/NAT	SUA Server	Use this screen to configure servers behind the HomeSafe.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Trigger Port	Use this screen to change your HomeSafe's trigger port settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.

**Table 2-17 Screens Summary**

LINK	TAB	FUNCTION
PARENTAL CONTROL	General	Use this screen to enable/disable parental control, configure idle timeout and group categories, register for content filtering service and edit user profiles.
	Bypass List	Use this screen to allow devices in your network access the Internet without using parental control.
FIREWALL	Settings	Use this screen to activate/deactivate the firewall and log packets related to firewall rules.
	Filter	This screen allows you to block sites containing certain keywords in the URL and set the days and times for the HomeSafe to perform content filtering.
	Services	Use this screen to enable service blocking.
REMOTE MGMT	TELNET	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the HomeSafe.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the HomeSafe.
	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the HomeSafe.
	SNMP	Use this screen to configure your HomeSafe's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the HomeSafe.
	Security	Use this screen to change your anti-probing settings.
UPnP	UPnP	Use this screen to enable UPnP on the HomeSafe.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your HomeSafe's log settings.
MAINTENANCE	Status	This screen contains administrative and system-related information.
	DHCP Table	This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
	Any IP	Use this screen to allow a computer to access the Internet without changing the network settings of the computer, when the IP addresses of the computer and the HomeSafe are not in the same subnet.
	F/W Upload	Use this screen to upload firmware to your HomeSafe.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your HomeSafe.
	Restart	This screen allows you to reboot the HomeSafe without turning the power off.
LOGOUT		Click this label to exit the web configurator.



## Chapter 3

# Connection Wizard

*This chapter provides information on the Connection Wizard screens in the main menu web configurator.*

### 3.1 Connection Wizard Overview

The web configurator's setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP for details on what to enter in each field. Leave a field blank if you don't have that information.

### 3.2 Connection Wizard : General Setup and System Name

**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the HomeSafe **System Name**.

#### 3.2.1 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the HomeSafe via DHCP.

Click **Next** to configure the HomeSafe for Internet access.

**Connection Wizard**

**General Setup:**

This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter a descriptive name for identification purposes. We recommend using your computer's name.

**System Name:**

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

**Domain Name:**

**Figure 3-1 Connection Wizard : General Setup**

### 3.3 Connection Wizard: Screen 2

Set up your wireless LAN using the second wizard screen.

**Connection Wizard**

**Wireless LAN Setup**

**ESSID**

**Choose Channel ID**

**Security**

**Figure 3-2 Connection Wizard : Wireless LAN Setup**

The following table describes the fields in this screen.

**Table 3-1 Connection Wizard : Wireless LAN Setup**

LABEL	DESCRIPTION
ESSID	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the HomeSafe, make sure all wireless stations use the same ESSID in order to access the network.
Choose Channel ID	To manually set the HomeSafe to use a channel, select a channel from the drop-down list box.

**Table 3-1 Connection Wizard : Wireless LAN Setup**

LABEL	DESCRIPTION
	<p>The level of <b>Security</b> can be selected as none, basic or extended. Choose <b>No</b> security to have no wireless LAN security configured and proceed to the <b>ISP Parameters for Internet Access</b> screen.</p> <p>Choose <b>Basic</b> security if you want to configure <b>WEP Encryption</b> parameters.</p> <p>Choose <b>Extend</b> security to configure a <b>Pre-Shared Key</b>.</p> <p>The third screen varies depending on which security level you select.</p>
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.



**The wireless stations and HomeSafe must use the same ESSID, channel ID and WEP encryption key (if WEP is enabled) for wireless communication.**

### 3.4 Connection Wizard : Screen 3

If you choose **Basic**, you can setup WEP Encryption parameters.

**Connection Wizard**

**Wireless LAN Setup**

**WEP Encryption** 64-bit WEP

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).  
 128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).  
 (Select one WEP key as an active key to encrypt wireless data transmission.)

☒ ASCII ☐ Hex

☒ Key 1

☐ Key 2

☐ Key 3

☐ Key 4

Back Next

**Figure 3-3 Connection Wizard: Wireless LAN Setup: Basic Security**

The following table describes the labels in this screen.

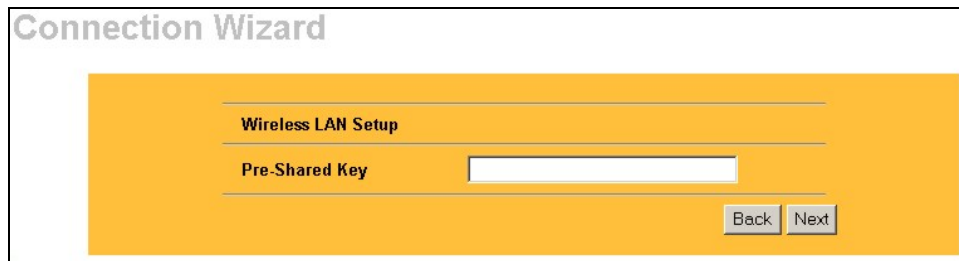
**Table 3-2 Connection Wizard: Wireless LAN Setup: Basic Security**

WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.



Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the HomeSafe and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose <b>64-bit WEP</b>, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose <b>128-bit WEP</b>, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

If you choose **Extend** security in the Wireless LAN Setup screen, you can set up a **Pre-Shared Key**.



**Figure 3-4 Connection Wizard: Wireless LAN Setup: Extend Security**

The following table describes the labels in this screen.

**Table 3-3 Connection Wizard: Wireless LAN Setup: Extend Security**

Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters.
Back	Click <b>Back</b> to display the previous screen.
Next	Click <b>Next</b> to proceed to the next screen.

Refer to the chapter on wireless LAN for more information.

## 3.5 Connection Wizard : Screen 4

The HomeSafe offers three choices of encapsulation. They are **Ethernet**, **PPP over Ethernet** or **PPTP**.

### 3.5.1 Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

**Connection Wizard**

**ISP Parameters for Internet Access**

Encapsulation: Ethernet

Service Type: Standard

User Name: N/A

Password: N/A

Login Server IP Address: N/A

Back Next

**Figure 3-5 Connection Wizard : Ethernet Encapsulation**

The following table describes the fields in this screen.

**Table 3-4 Connection Wizard : Ethernet Encapsulation**

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet. Otherwise, choose <b>PPP over Ethernet</b> or <b>PPTP</b> for a dial-up connection.
Service Type	Choose from <b>Standard</b> , <b>Telstra</b> (RoadRunner Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method), <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method) or <b>Telia Login</b> . The following fields are not applicable ( <b>N/A</b> ) for the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select <b>Telia Login</b> in the <b>Service Type</b> field. Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Every (min)	This field only applies when you select <b>Telia Login</b> in the <b>Service Type</b> field. The Telia server logs the HomeSafe out if the HomeSafe does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the HomeSafe to wait between logins.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

### 3.5.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

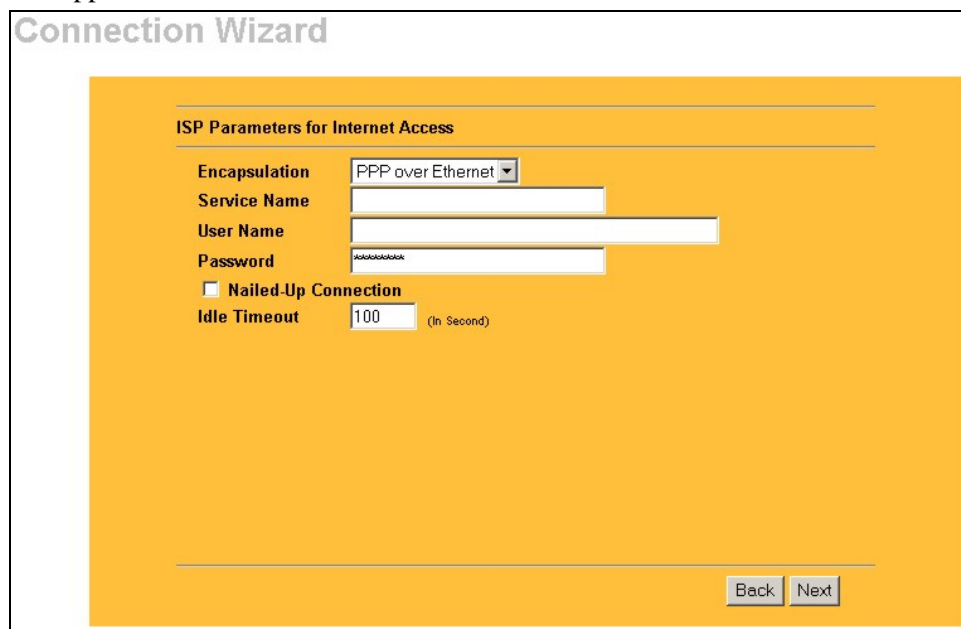
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the HomeSafe (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the HomeSafe does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.



**Figure 3-6 Connection Wizard : PPPoE Encapsulation**

The following table describes the fields in this screen.

**Table 3-5 Connection Wizard : PPPoE Encapsulation**

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose <b>PPP over Ethernet</b> from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.

**Table 3-5 Connection Wizard : PPPoE Encapsulation**

LABEL	DESCRIPTION
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is <b>100</b> seconds.
Next	Click <b>Next</b> to continue.
Back	Click <b>Back</b> to return to the previous screen.

### 3.5.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.



**The HomeSafe supports one PPTP server connection at any given time.**

**Figure 3-7 Connection Wizard : PPTP Encapsulation**

The following table describes the fields in this screen.

**Table 3-6 Connection Wizard : PPTP Encapsulation**

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select <b>PPTP</b> from the drop-down list box.

**Table 3-6 Connection Wizard : PPTP Encapsulation**

LABEL	DESCRIPTION
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 100 seconds.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

## 3.6 Connection Wizard : Screen 5

The fifth wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

### 3.6.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

**Table 3-7 Private IP Address Ranges**

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.



**Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.**

---

### 3.6.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your HomeSafe, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your HomeSafe will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the HomeSafe unless you are instructed to do otherwise.

### 3.6.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of [www.zyxel.com](http://www.zyxel.com) is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The HomeSafe can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
2. If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

### 3.6.4 WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

**Table 3-8 Example of Network Properties for LAN Servers with Fixed IP Addresses**

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(HomeSafe LAN IP)

The fifth wizard screen varies according to the type of encapsulation that you select in the third wizard screen.

**Figure 3-8 Connection Wizard : WAN Setup**

The following table describes the fields in this screen.

**Table 3-9 Connection Wizard : WAN Setup**

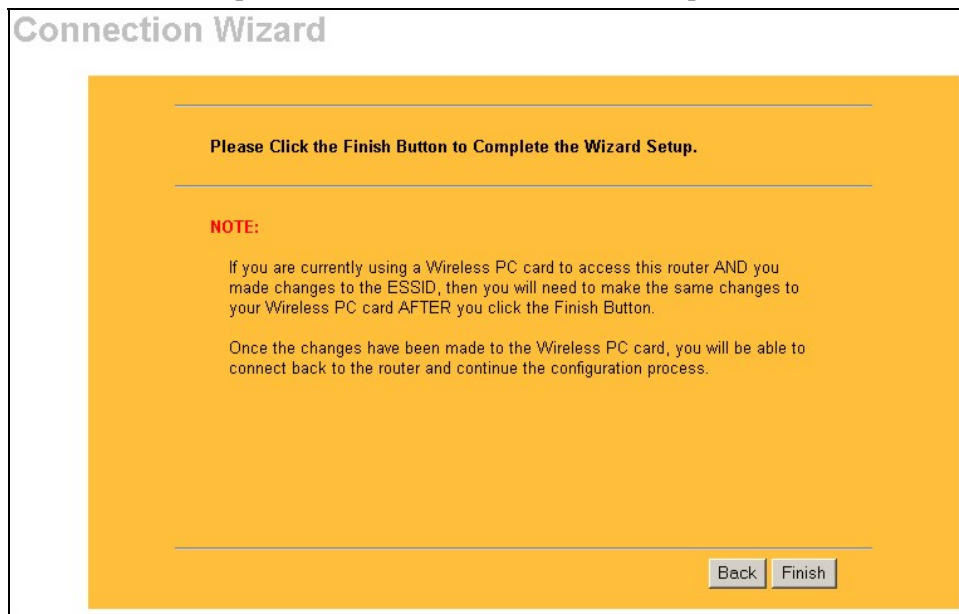
LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Type your network's IP Subnet Mask.
DNS Server Address Assignment (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The HomeSafe uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	

**Table 3-9 Connection Wizard : WAN Setup**

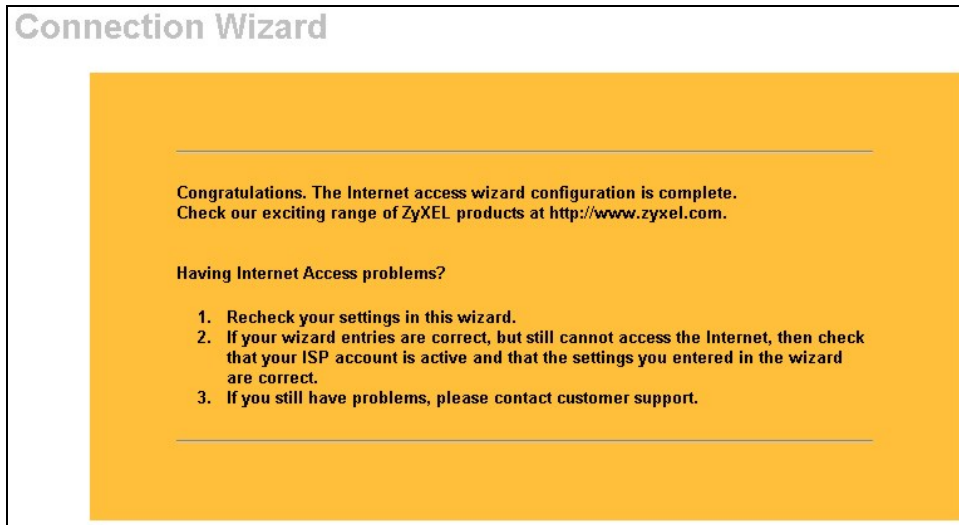
LABEL	DESCRIPTION
First DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the HomeSafe's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.  Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.  Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Second DNS Server	
Third DNS Server	
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

### 3.7 Basic Setup Complete

Click **Back** to return to the previous screen or click **Finish** to complete and save the wizard setup.

**Figure 3-9 Connection Wizard Finish**





**Figure 3-10 Connection Wizard Problems**

Well done! You have successfully set up your HomeSafe to operate on your network and access the Internet.



---

---

## Part II:

---

### System, LAN, WLAN and WAN

---

This part covers configuration of the system, LAN, WLAN and WAN screens.

# Chapter 4

## System Screens

*This chapter provides information on the System screens.*

### 4.1 System Overview

See the *Wizard Setup* chapter for more information on the next few screens.

### 4.2 Configuring General Setup

Click **SYSTEM** to open the **General** screen.

**Figure 4-1 SYSTEM : General Setup**

The following table describes the labels in this screen.

**Table 4-1 SYSTEM : General Setup**

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field (see the <i>Wizard Setup</i> chapter for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The HomeSafe uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	

**Table 4-1 SYSTEM : General Setup**

LABEL	DESCRIPTION
First DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the HomeSafe's WAN IP address). The field below displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field below. If you chose <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> . If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b> .
Third DNS Server	Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 4.3 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](http://www.dyndns.org). This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

### 4.3.1 DynDNS Wildcard

Enabling the wildcard feature for your host causes \*.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, [www.yourhost.dyndns.org](http://www.yourhost.dyndns.org) and still reach your hostname.



**If you have a private WAN IP address, then you cannot use Dynamic DNS.**

---

## 4.4 Configuring Dynamic DNS

To change your HomeSafe's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

Figure 4-2 SYSTEM : DDNS

The following table describes the labels in this screen.

Table 4-2 SYSTEM : DDNS

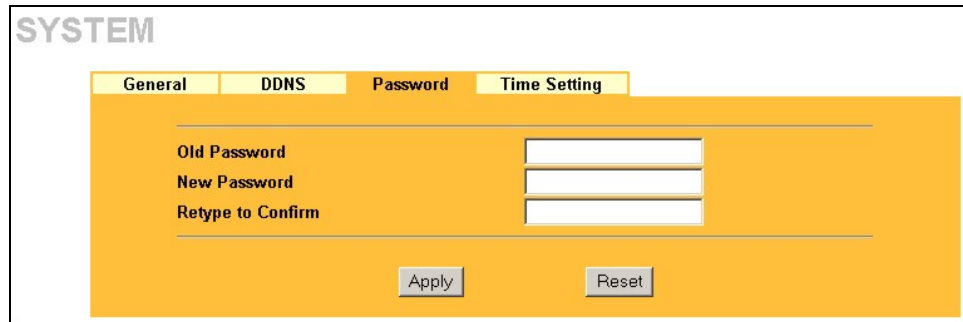
LABEL	DESCRIPTION
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option (Only applies to custom DNS)	This option is available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address of the HomeSafe.
DDNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
User specified IP Address	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Addr	Enter the IP address if you select the <b>User Specify</b> option.

**Table 4-2 SYSTEM : DDNS**

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 4.5 Configuring Password

To change your HomeSafe's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the HomeSafe's password.

**Figure 4-3 SYSTEM : Password**

The following table describes the labels in this screen.

**Table 4-3 SYSTEM : Password**

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 4.6 Configuring Time Setting

To change your HomeSafe's time and date, click **SYSTEM**, then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the HomeSafe's time based on your local time zone.

Figure 4-4 SYSTEM : Time Setting

The following table describes the labels in this screen.

Table 4-4 SYSTEM : Time Setting

LABEL	DESCRIPTION
Time Protocol	<p>Select the time service protocol that your time server sends when you turn on the HomeSafe. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.</p> <p>The main difference between them is the format.</p> <p><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, <b>NTP (RFC 1305)</b>, is similar to Time (RFC 868).</p> <p>Select <b>None</b> to enter the time and date manually.</p>
Time Server IP Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	<p>This field displays the time of your HomeSafe.</p> <p>Each time you reload this page, the HomeSafe synchronizes the time with the time server.</p>
New Time	<p>This field displays the last updated time from the time server.</p> <p>When you select <b>None</b> in the <b>Time Protocol</b> field, enter the new time in this field and then click <b>Apply</b>.</p>
Current Date	<p>This field displays the date of your HomeSafe.</p> <p>Each time you reload this page, the HomeSafe synchronizes the date with the time server.</p>
New Date	<p>This field displays the last updated date from the time server.</p> <p>When you select <b>None</b> in the <b>Time Protocol</b> field, enter the new date in this field and then click <b>Apply</b>.</p>
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).



**Table 4-4 SYSTEM : Time Setting**

<b>LABEL</b>	<b>DESCRIPTION</b>
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected <b>Daylight Savings</b> .
End Date	Enter the month and day that your daylight-savings time ends on if you selected <b>Daylight Savings</b> .
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Chapter 5

## LAN Screens

*This chapter describes how to configure LAN settings.*

### 5.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

### 5.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the HomeSafe as a DHCP server or disable it. When configured as a server, the HomeSafe provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

#### 5.2.1 IP Pool Setup

The HomeSafe is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the HomeSafe itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

#### 5.2.2 System DNS Servers

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter.

### 5.3 LAN TCP/IP

The HomeSafe has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

#### 5.3.1 Factory LAN Defaults

The LAN parameters of the HomeSafe are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

#### 5.3.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

#### 5.3.3 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP

packets. When set to **Both** or **Out Only**, the HomeSafe will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

**RIP Version** controls the format and the broadcasting method of the RIP packets that the HomeSafe sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

### 5.3.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The HomeSafe supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the HomeSafe queries all directly connected networks to gather group membership. After that, the HomeSafe periodically updates this information. IP multicasting can be enabled/disabled on the HomeSafe LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

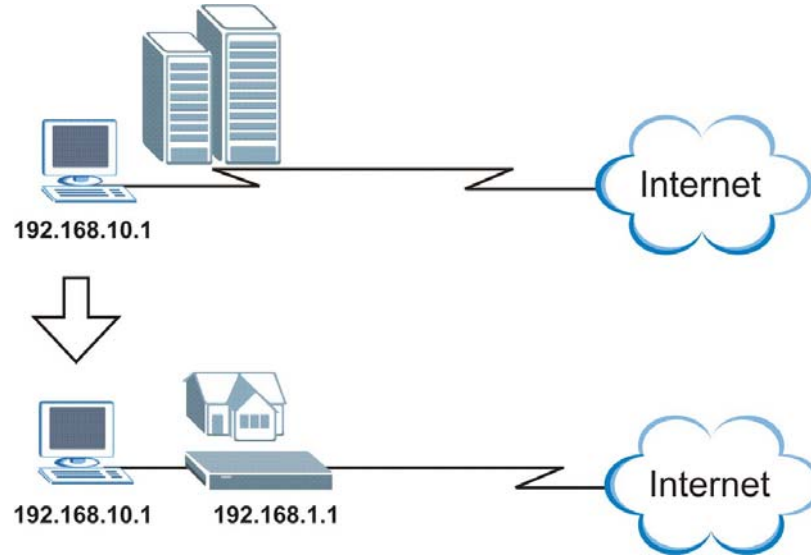
## 5.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the HomeSafe to be in the same subnet to allow the computer to access the Internet (through the HomeSafe). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the HomeSafe.

With the Any IP feature and NAT enabled, the HomeSafe allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the HomeSafe are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the HomeSafe and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a HomeSafe is installed, you can still

use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the HomeSafe are not in the same subnet.



**Figure 5-1 Any IP Example Application**

The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the HomeSafe's IP address.



**You *must* enable NAT/SUA to use the Any IP feature on the HomeSafe.**

### 5.4.1 How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the HomeSafe) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the HomeSafe.

1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the HomeSafe) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The HomeSafe receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the HomeSafe.
5. When the HomeSafe receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the HomeSafe and the Internet as if it is in the same subnet as the HomeSafe.

## 5.5 Configuring IP

Click **LAN** to open the **IP** screen.

**Figure 5-2 LAN : IP**

The following table describes the fields in this screen.

**Table 5-1 LAN : IP**

LABEL	DESCRIPTION
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the <b>DHCP Server</b> check box selected unless your ISP instructs you to do otherwise. Clear it to disable the HomeSafe acting as a DHCP server. When configured as a server, the HomeSafe provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Servers Assigned by DHCP Server The HomeSafe passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The HomeSafe only passes this information to the LAN DHCP clients when you select the <b>DHCP Server</b> check box. When you clear the <b>DHCP Server</b> check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.	

Table 5-1 LAN : IP

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the HomeSafe's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>DNS Relay</b> to have the HomeSafe act as a DNS proxy. The HomeSafe's LAN IP address displays in the field to the right (read-only). The HomeSafe tells the DHCP clients on the LAN that the HomeSafe itself is the DNS server. When a computer on the LAN sends a DNS query to the HomeSafe, the HomeSafe forwards the query to the HomeSafe's system DNS server (configured in the <b>SYSTEM General</b> screen) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
LAN TCP/IP	
IP Address	Type the IP address of your HomeSafe in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your HomeSafe will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the HomeSafe 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the HomeSafe will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the HomeSafe sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Any IP Setup	

**Table 5-1 LAN : IP**

LABEL	DESCRIPTION
Active	Select this option to activate the Any-IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the HomeSafe are not in the same subnet.  When you disable the Any-IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the HomeSafe's LAN IP address can connect to the HomeSafe or access the Internet through the HomeSafe.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow from LAN to WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.  Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.6 Configuring Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your HomeSafe's Static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

#	MAC Address	IP Address
1	00:50:8D:48:59:1F	192.168.1.33
2		0.0.0.0
3		0.0.0.0
4		0.0.0.0
5		0.0.0.0
6		0.0.0.0
7		0.0.0.0
8		0.0.0.0

**Figure 5-3 LAN : Static DHCP**

The following table describes the labels in this screen.

**Table 5-2 LAN : Static DHCP**

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.7 Configuring IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The HomeSafe supports three logical LAN interfaces via its single physical Ethernet interface with the HomeSafe itself as the gateway for each LAN network.

To change your HomeSafe's IP Alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

The screenshot shows the 'LAN IP SETUP' window with three tabs: 'IP', 'Static DHCP', and 'IP Alias'. The 'IP Alias' tab is selected. It contains two sections for 'IP Alias 1' and 'IP Alias 2'. Each section has a checkbox, an 'IP Address' field (0.0.0.0), an 'IP Subnet Mask' field (0.0.0.0), a 'RIP Direction' dropdown (None), and a 'RIP Version' dropdown (RIP-1). At the bottom are 'Apply' and 'Reset' buttons.

**Figure 5-4 LAN : IP Alias**

The following table describes the labels in this screen.

**Table 5-3 LAN : IP Alias**

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the HomeSafe.
IP Address	Enter the IP address of your HomeSafe in dotted decimal notation.
IP Subnet Mask	Your HomeSafe will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the HomeSafe.



**Table 5-3 LAN : IP Alias**

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the HomeSafe will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the HomeSafe sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Chapter 6

## Wireless Configuration and Roaming

*This chapter discusses how to configure the Wireless and Roaming screens on the HomeSafe.*

### 6.1 Wireless LAN Overview

This section introduces the wireless LAN(WLAN) and some basic scenarios.

#### 6.1.1 IBSS

An Independent Basic Service Set (IBSS), also called an Ad-hoc network, is the simplest WLAN configuration. An IBSS is defined as two or more computers with wireless adapters within range of each other that form an independent (wireless) network without the need of an access point (AP).



**Figure 6-1 IBSS (Ad-hoc) Wireless LAN**

#### 6.1.2 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

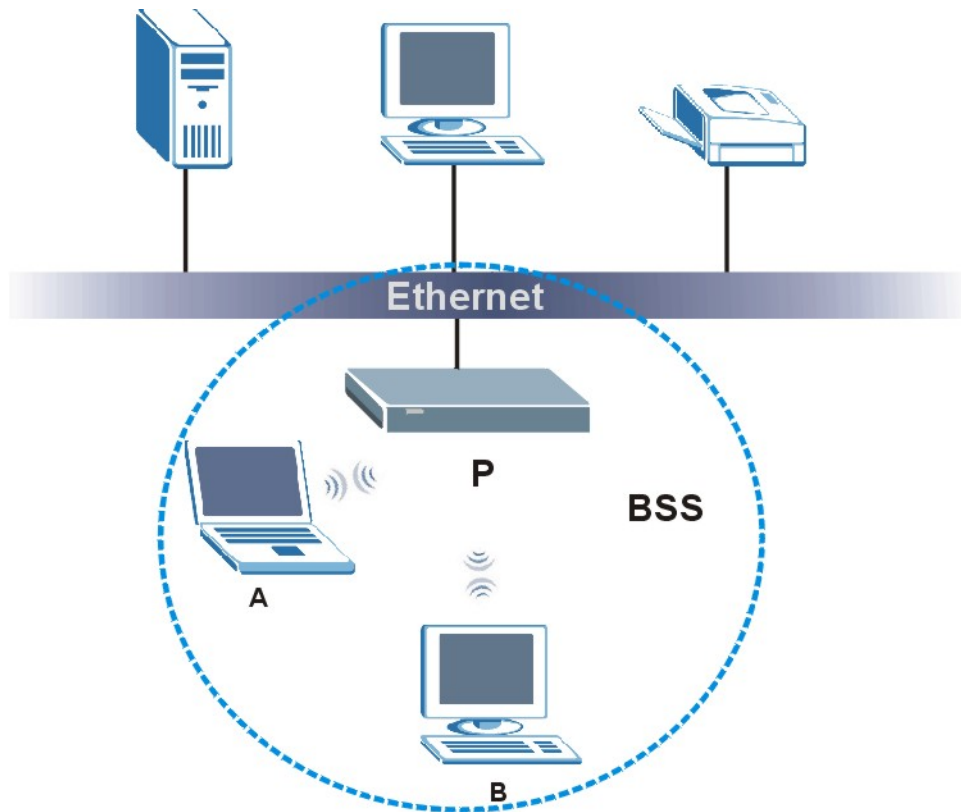


Figure 6-2 Basic Service set

### 6.1.3 ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

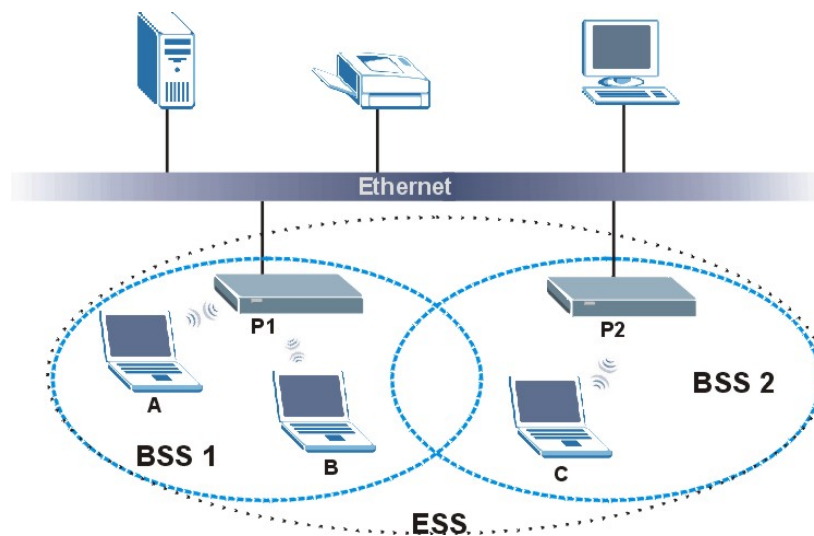


Figure 6-3 Extended Service Set

## 6.2 Wireless LAN Basics

Refer also to the *Wizard Setup* chapter for more background information on Wireless LAN features, such as channels.

### 6.2.1 RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot “hear” each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

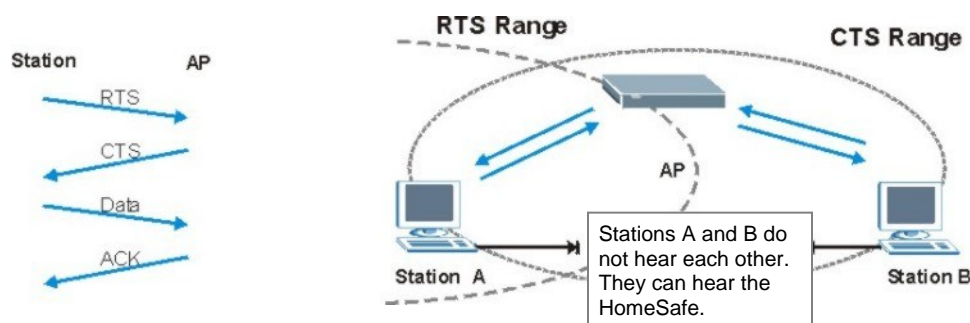


Figure 6-4 RTS/CTS

When station A sends data to the HomeSafe, it might not know that station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the “cost” of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.



**Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.**

---

### 6.2.2 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the HomeSafe will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set, then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## 6.3 Configuring Wireless

---



**If you are configuring the HomeSafe from a computer connected to the wireless LAN and you change the HomeSafe's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the HomeSafe's new settings.**

---

Click the **WIRELESS** link under **ADVANCED** to open the **Wireless** screen.

**WIRELESS LAN**

Wireless | MAC Filter | Roaming | Local User Database | RADIUS

☒ Enable Wireless LAN

ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: No Security

Preamble: Long

802.11 Mode: Mixed


Max. Frame Burst: 650 (0 ~ 1800)

Apply | Reset

**Figure 6-5 WLAN : Wireless**

The following table describes the general wireless LAN labels in this screen.

Table 6-1 WLAN : Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
ESSID	<p>(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <hr/> <p> <b>If you are configuring the HomeSafe from a computer connected to the wireless LAN and you change the HomeSafe's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the HomeSafe's new settings.</b></p> <hr/>
Hide ESSID	Select this check box to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning using a site survey tool.
Choose Channel ID	<p>Set the operating frequency/channel depending on your particular region.</p> <p>Select a channel from the drop-down list box.</p> <p>Refer to the <i>Wizard Setup</i> chapter for more information on channels.</p>
RTS/CTS Threshold	Enter a value between 0 and 2432. The default is <b>2432</b> .
Fragmentation Threshold	Enter a value between 256 and 2432. The default is <b>2432</b> . It is the maximum data fragment size that can be sent.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

See the *Wireless Security* chapter for information on the other labels in this screen.

## 6.4 Configuring Roaming

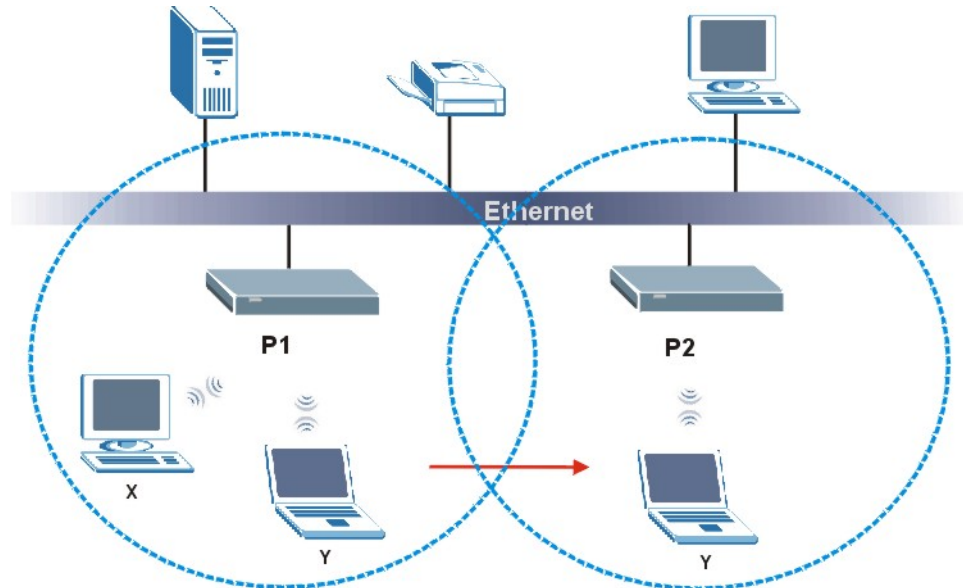
A wireless station is a device with an IEEE 802.11 compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in *Figure 6-6*.

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless

station may not be able to communicate with other wireless stations on the network and vice versa.



**Figure 6-6 Roaming Example**

The steps below describe the roaming process.

1. As wireless station **Y** moves from the coverage area of access point **P1** to that of access point **P2**, it scans and uses the signal of access point **P2**.
2. Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.
3. Access point **P1** updates the new position of wireless station.
4. Wireless station **Y** sends a request to access point **P2** for re-authentication.

#### **6.4.1 Requirements for Roaming**

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your HomeSafe, click the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

WIRELESS LAN

Wireless

MAC Filter

Roaming

Local User Database

RADIUS

Roaming Configuration

Active

No

Port

3517


Apply

Reset

Figure 6-7 WLAN : Roaming

The following table describes the labels in this screen.

Table 6-2 WLAN : Roaming

LABEL	DESCRIPTION
Active	<p>Select <b>Yes</b> from the drop-down list box to enable roaming on the HomeSafe if you have two or more HomeSafes on the same subnet.</p> <hr/> <p> <b>All APs on the same subnet and the wireless stations must have the same ESSID to allow roaming.</b></p> <hr/>
Port	Enter the port number to communicate roaming information between APs. The port number must be the same on all APs. The default is 3517. Make sure this port is not used by other services.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.





# Chapter 7

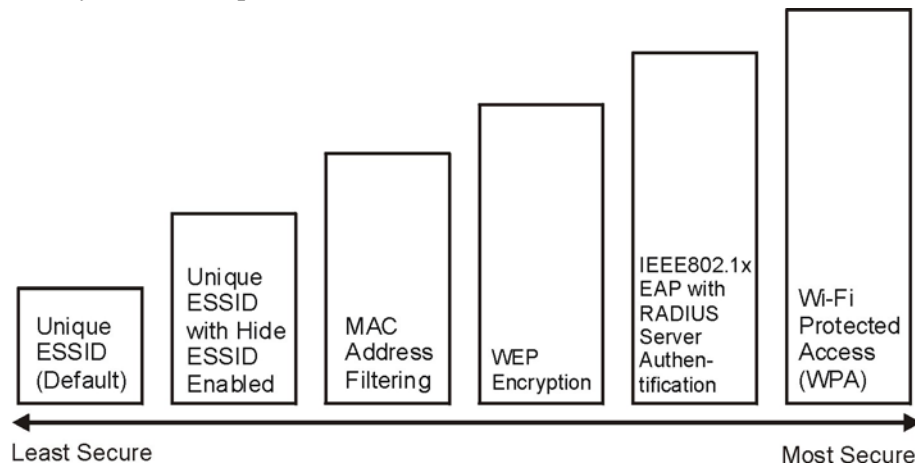
## Wireless Security

*This Chapter describes how to use the MAC Filter, 802.1x, Local User Database and RADIUS to configure wireless security on your HomeSafe.*

### 7.1 Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network.

The figure below shows the possible wireless security levels on your HomeSafe. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.



**Figure 7-1 HomeSafe Wireless Security Levels**

If you do not enable any wireless security on your HomeSafe, your network is accessible to any wireless networking device that is within range.

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

**WIRELESS LAN**

Wireless    MAC Filter    Roaming    Local User Database    RADIUS

☒ Enable Wireless LAN

ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: No Security

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~ 1800)

Apply    Reset

Figure 7-2 WLAN : Wireless : No Security

The following table describes the labels in this screen.

Table 7-1 WLAN : Wireless : No Security

LABEL	DESCRIPTION
Security	<p>Choose from one of the security features listed in the drop-down box.</p> <ul style="list-style-type: none"> <li>➤ No Security</li> <li>➤ Static WEP</li> <li>➤ WPA-PSK</li> <li>➤ WPA</li> <li>➤ 802.1x + Dynamic WEP</li> <li>➤ 802.1x + Static WEP</li> <li>➤ 802.1x + No WEP</li> </ul>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are <b>Long</b>, <b>Short</b> and <b>Dynamic</b>. The default setting is <b>Long</b>.</p> <p>See the section on preamble for more information.</p>
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.</p>
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.</p>
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.

Table 7-1 WLAN : Wireless : No Security

LABEL	DESCRIPTION
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.2 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 7-2 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

## 7.3 WEP Overview

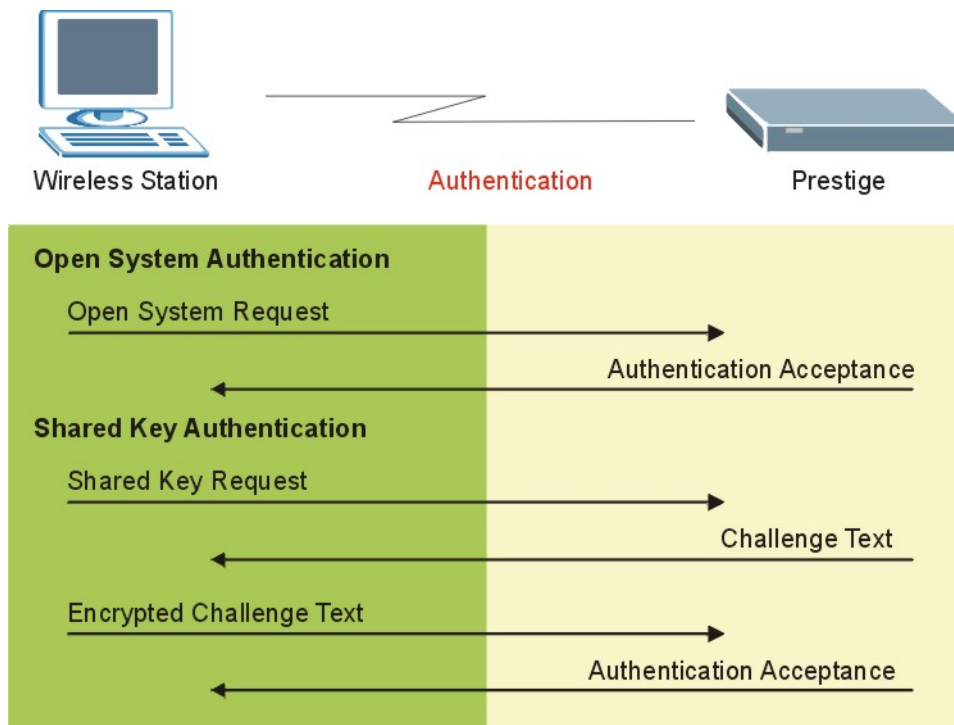
WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication.

### 7.3.1 Data Encryption

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your HomeSafe allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

### 7.3.2 Authentication

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.



**Figure 7-3 WEP Authentication Steps**

Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your HomeSafe's authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the HomeSafe will accept either type of authentication request and the HomeSafe will fall back to use open authentication if the shared key does not match.

### 7.3.3 Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless clients support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless clients support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the HomeSafe and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the HomeSafe automatically use short preamble when all wireless clients support it, otherwise the HomeSafe uses long preamble.



**The HomeSafe and the wireless stations MUST use the same preamble mode in order to communicate.**

## 7.4 Configuring WEP Encryption

In order to configure and enable WEP encryption; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **Static WEP** from the **Security** list.

The screenshot shows the 'WIRELESS LAN' configuration interface. At the top, there are tabs for 'Wireless', 'MAC Filter', 'Roaming', 'Local User Database', and 'RADIUS'. The 'Wireless' tab is active. Below the tabs, there is a section for 'Enable Wireless LAN' with a checked checkbox. The 'ESSID' field is set to 'Wireless'. There is a 'Hide ESSID' checkbox which is unchecked. The 'Choose Channel ID' dropdown is set to 'Channel-06 2437MHz'. The 'RTS/CTS Threshold' and 'Fragmentation Threshold' are both set to '2432'. The 'Security' dropdown is set to 'Static WEP'. The 'WEP Encryption' dropdown is set to '64-bit WEP'. The 'Authentication Method' dropdown is set to 'Auto'. Below this, there are radio buttons for 'ASCII' and 'Hex', with 'ASCII' selected. There are four 'Key' fields (Key 1, Key 2, Key 3, Key 4) with input boxes. The 'Preamble' dropdown is set to 'Long'. The '802.11 Mode' dropdown is set to 'Mixed'. The 'Max. Frame Burst' field is set to '650'. At the bottom, there are 'Apply' and 'Reset' buttons. A red circle highlights the 'Security', 'WEP Encryption', 'Authentication Method', 'Key' fields, and 'Preamble' section.

**Figure 7-4 WLAN : Wireless : Static WEP Encryption**

The following table describes the wireless LAN security labels in this screen.

**Table 7-3 WLAN : Wireless : Static WEP Encryption**

LABEL	DESCRIPTION
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Authentication Method	This field is activated when you select <b>64-bit WEP</b> or <b>128-bit WEP</b> in the <b>WEP Encryption</b> field. Select <b>Auto</b> , <b>Open System</b> or <b>Shared Key</b> from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option in order to enter hexadecimal characters as the WEP keys. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

**Table 7-3 WLAN : Wireless : Static WEP Encryption**

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the HomeSafe and the wireless stations must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> and <b>Dynamic</b> . The default setting is <b>Dynamic</b> . See the section on preamble for more information.
802.11 Mode	Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe. Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe. Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.5 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

### 7.5.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the HomeSafe's Local User Database for WPA authentication purposes since the Local User Database uses EAP MD5, which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

### 7.5.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

### 7.5.3 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

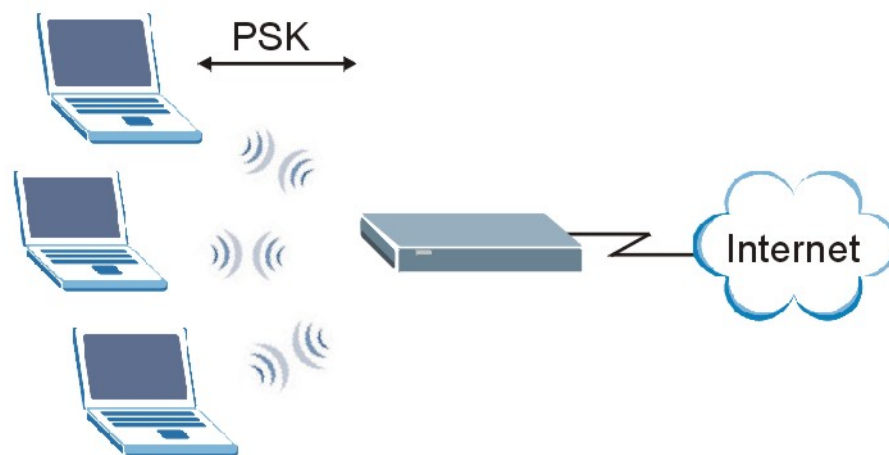


Figure 7-5 WPA - PSK Authentication



## 7.6 Configuring WPA-PSK Authentication


In order to configure and enable WPA-PSK Authentication; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **WPA-PSK** from the **Security** list.

The screenshot shows the 'WIRELESS LAN' configuration interface. At the top, there are tabs for 'Wireless', 'MAC Filter', 'Roaming', 'Local User Database', and 'RADIUS'. The 'Wireless' tab is selected. Below the tabs, there is a section for 'Enable Wireless LAN' with a checked checkbox. The 'ESSID' is set to 'Wireless'. There is an unchecked checkbox for 'Hide ESSID'. The 'Choose Channel ID' is set to 'Channel-06 2437MHz'. The 'RTS/CTS Threshold' and 'Fragmentation Threshold' are both set to '2432'. The 'Security' dropdown is set to 'WPA-PSK'. The 'Pre-Shared Key' field is empty. The 'ReAuthentication Timer' is set to '1800' (In Seconds). The 'Idle Timeout' is set to '3600' (In Seconds). The 'WPA Group Key Update Timer' is set to '1800' (In Seconds). The 'Preamble' is set to 'Long'. The '802.11 Mode' is set to 'Mixed'. The 'Max. Frame Burst' is set to '650'. At the bottom, there are 'Apply' and 'Reset' buttons.

**Figure 7-6 WLAN : Wireless : WPA-PSK**

The following table describes the labels in this screen.

**Table 7-4 WLAN : Wireless : WPA-PSK**

LABEL	DESCRIPTION
Pre-Shared Key	The encryption mechanisms used for <b>WPA</b> and <b>WPA-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  <div style="text-align: center;">  <p><b>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</b></p> </div>
Idle Timeout	The HomeSafe automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

**Table 7-4 WLAN : Wireless : WPA-PSK**

<b>LABEL</b>	<b>DESCRIPTION</b>
WPA Group Key Update Timer	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or <b>RADIUS</b> server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode. The HomeSafe default is <b>1800</b> seconds (30 minutes).
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> or <b>Dynamic</b> . The default setting is <b>Long</b> . See the section on preamble for more information.
802.11 Mode	Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe. Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe. Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.7 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The AEGIS client is bundled free (at the time of writing) with the HomeSafe client adaptor(s). The XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it. Funk's client runs supports a wider variety of authentication protocols than the Windows XP patch, but you need to buy it.

### 7.7.1 WPA with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically

generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

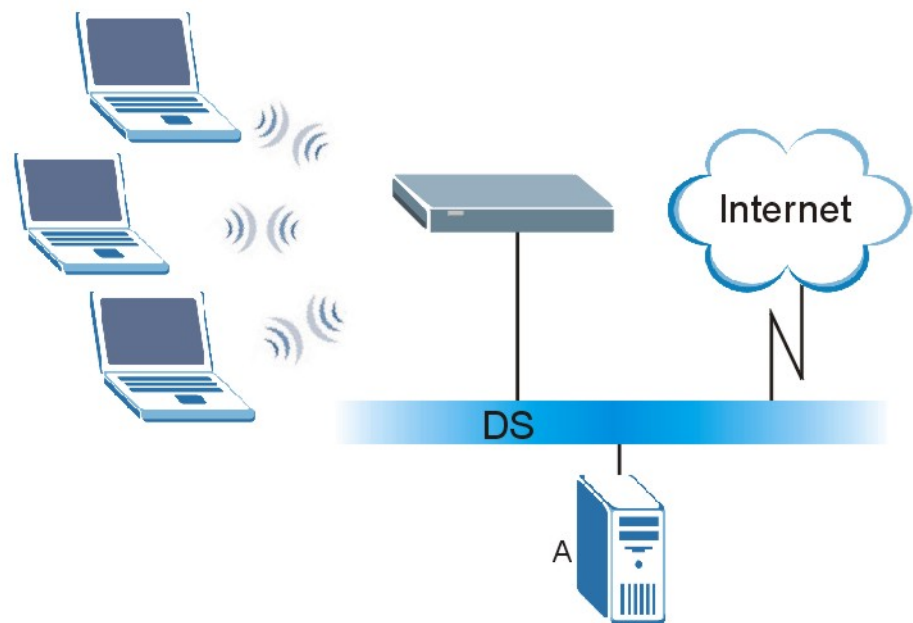


Figure 7-7 WPA with RADIUS Application Example

## 7.8 Configuring WPA Authentication

In order to configure and enable WPA Authentication; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **WPA** from the **Security** list.


**WIRELESS LAN**

Wireless	MAC Filter	Roaming	Local User Database	RADIUS
<input checked="" type="checkbox"/> <b>Enable Wireless LAN</b>				
ESSID		Wireless		
<input type="checkbox"/> <b>Hide ESSID</b>				
Choose Channel ID		Channel-06 2437MHz		
RTS/CTS Threshold		2432 (0 ~ 2432)		
Fragmentation Threshold		2432 (256 ~ 2432)		
Security		WPA		
ReAuthentication Timer		1800 (In Seconds)		
Idle Timeout		3600 (In Seconds)		
WPA Group Key Update Timer		1800 (In Seconds)		
Preamble		Long		
802.11 Mode		Mixed		
Max. Frame Burst		650 (0 ~ 1800)		
<div>Apply Reset</div>				

Figure 7-8 Wireless: WPA

The following table describes the labels in this screen.

**Table 7-5 WLAN : Wireless : WPA**

<b>LABEL</b>	<b>DESCRIPTION</b>
ReAuthentication Timer (in seconds)	<p>Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <hr/> <p> <b>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</b></p> <hr/>
Idle Timeout	The HomeSafe automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
WPA Group Key Update Timer	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or <b>RADIUS</b> server (if using WPA key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode. The HomeSafe default is <b>1800</b> seconds (30 minutes).
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> or <b>Dynamic</b> . The default setting is <b>Long</b> . See the section on preamble for more information.
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.</p>
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.</p>
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.9 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the HomeSafe (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

See also the section on RADIUS in this *User's Guide*.

## 7.10 Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

To use Dynamic WEP, enable and configure the RADIUS server (see *section 7.17*) and enable Dynamic WEP Key Exchange in the Wireless screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP



**EAP-MD5 cannot be used with Dynamic WEP Key Exchange.**

## 7.11 Configuring 802.1x and Dynamic WEP Key Exchange

In order to configure and enable 802.1x and Dynamic WEP Key Exchange; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + Dynamic WEP** from the **Security** list.

**WIRELESS LAN**

Wireless | MAC Filter | Roaming | Local User Database | RADIUS

☒ Enable Wireless LAN

ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: 802.1x + Dynamic WEP

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Dynamic WEP Key Exchange: 64-bit WEP

Preamble: Long

802.11 Mode: Mixed


Max. Frame Burst: 650 (0 ~ 1800)

Apply Reset

**Figure 7-9 WLAN : Wireless : 802.1x and Dynamic WEP**

The following table describes the labels in this screen.

**Table 7-6 WLAN : Wireless : 802.1x and Dynamic WEP**

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	<p>Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <hr/> <p> <b>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</b></p> <hr/>
Idle Timeout	The HomeSafe automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Dynamic WEP Key Exchange	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption. Up to 32 stations can access the HomeSafe when you configure dynamic WEP key exchange. This field is not available when you set <b>Security</b> to <b>WPA</b> or <b>WPA-PSK</b> .
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> or <b>Dynamic</b> . The default setting is <b>Long</b> . See the section on preamble for more information.
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.</p>
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.</p>
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.12 Configuring 802.1x and Static WEP Key Exchange

In order to configure and enable 802.1x and Static WEP Key Exchange; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + Static WEP** from the **Security** list.

**WIRELESS LAN**

Wireless | MAC Filter | Roaming | Local User Database | RADIUS

☒ Enable Wireless LAN

ESSID: Wireless

☐ Hide ESSID

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Security: 802.1x + Static WEP

WEP Encryption: 64-bit WEP

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).  
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).  
(Select one WEP key as an active key to encrypt wireless data transmission.)

☒ ASCII ☐ Hex

☒ Key 1: [ ]  
☐ Key 2: [ ]  
☐ Key 3: [ ]  
☐ Key 4: [ ]

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Authentication Databases: Local User Database Only

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~ 1800)

Apply Reset

Figure 7-10 WLAN : Wireless : 802.1x and Static WEP


The following table describes the labels in this screen.

Table 7-7 WLAN : Wireless : 802.1x and Static WEP

LABEL	DESCRIPTION
WEP Encryption	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Authentication Method	This field is activated when you select <b>64-bit WEP</b> or <b>128-bit WEP</b> in the WEP Encryption field. Select Auto, Open System or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option in order to enter hexadecimal characters as the WEP keys. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the HomeSafe and the wireless stations must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.



**Table 7-7 WLAN : Wireless : 802.1x and Static WEP**

LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	<p>Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).</p> <hr/> <p> <b>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</b></p> <hr/>
Idle Timeout	<p>The HomeSafe automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).</p>
Authentication Databases	<p>The authentication database contains wireless station login information. The local user database is the built-in database on the HomeSafe. The RADIUS is an external server. Use this drop-down list box to select which database the HomeSafe should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select <b>Local User Database Only</b> to have the HomeSafe just check the built-in user database on the HomeSafe for a wireless station's username and password.</p> <p>Select <b>RADIUS Only</b> to have the HomeSafe just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select <b>Local first, then RADIUS</b> to have the HomeSafe first check the user database on the HomeSafe for a wireless station's username and password. If the user name is not found, the HomeSafe then checks the user database on the specified RADIUS server.</p> <p>Select <b>RADIUS first, then Local</b> to have the HomeSafe first check the user database on the specified RADIUS server for a wireless station's username and password. If the HomeSafe cannot reach the RADIUS server, the HomeSafe then checks the local user database on the HomeSafe. When the user name is not found or password does not match in the RADIUS server, the HomeSafe will not check the local user database and the authentication fails.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are <b>Long</b>, <b>Short</b> or <b>Dynamic</b>. The default setting is <b>Long</b>. See the section on preamble for more information.</p>
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.</p>
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the HomeSafe.</p>



**Table 7-7 WLAN : Wireless : 802.1x and Static WEP**

LABEL	DESCRIPTION
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.13 Configuring 802.1x

In order to configure and enable 802.1x; click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. Select **802.1x + No WEP** from the **Security** list.

**Figure 7-11 WLAN : Wireless: 802.1x**

The following table describes the labels in this screen.

**Table 7-8 WLAN : Wireless: 802.1x**


LABEL	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes).  <div style="text-align: center;">  <p><b>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</b></p> </div>
Idle Timeout	The HomeSafe automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 7-8 WLAN : Wireless: 802.1x

LABEL	DESCRIPTION
Authentication Databases	<p>The authentication database contains wireless station login information. The local user database is the built-in database on the HomeSafe. The RADIUS is an external server. Use this drop-down list box to select which database the HomeSafe should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select <b>Local User Database Only</b> to have the HomeSafe just check the built-in user database on the HomeSafe for a wireless station's username and password.</p> <p>Select <b>RADIUS Only</b> to have the HomeSafe just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select <b>Local first, then RADIUS</b> to have the HomeSafe first check the user database on the HomeSafe for a wireless station's username and password. If the user name is not found, the HomeSafe then checks the user database on the specified RADIUS server.</p> <p>Select <b>RADIUS first, then Local</b> to have the HomeSafe first check the user database on the specified RADIUS server for a wireless station's username and password. If the HomeSafe cannot reach the RADIUS server, the HomeSafe then checks the local user database on the HomeSafe. When the user name is not found or password does not match in the RADIUS server, the HomeSafe will not check the local user database and the authentication fails.</p>
Preamble	<p>Select a preamble type from the drop-down list menu. Choices are <b>Long</b>, <b>Short</b> or <b>Dynamic</b>. The default setting is <b>Long</b>. See the section on preamble for more information.</p>
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.</p>
Max. Frame Burst	<p>Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the HomeSafe transmits IEEE 802.11g wireless traffic only.</p> <p>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. The default is 650.</p>
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.14 MAC Filter

The MAC filter screen allows you to configure the HomeSafe to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the HomeSafe (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your HomeSafe's MAC filter settings, click the **WIRELESS** link under **ADVANCED** and then the **MAC Filter** tab. The screen appears as shown.

**WIRELESS LAN**

Wireless   **MAC Filter**   Roaming   Local User Database   RADIUS

---

**MAC Address Filter**

Active

Filter Action

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

Apply   Reset

Figure 7-12 WLAN : MAC Address Filter

The following table describes the labels in this menu.

Table 7-9 WLAN : MAC Address Filter

LABEL	DESCRIPTION
Active	Select <b>Yes</b> from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the <b>MAC Address</b> table. Select <b>Deny Association</b> to block access to the HomeSafe, MAC addresses not listed will be allowed to access the HomeSafe Select <b>Allow Association</b> to permit access to the HomeSafe, MAC addresses not listed will be denied access to the HomeSafe.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the HomeSafe in these address fields.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.15 Introduction to Local User Database

By storing user profiles locally on the HomeSafe, your HomeSafe is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way. You can only use **Local User Database** with 802.1x key management protocol.

## 7.16 Configuring Local User Database

To change your HomeSafe's local user database, click the **WIRELESS** link under **ADVANCED** and then the **Local User Database** tab. The screen appears as shown.

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		
13	<input type="checkbox"/>		
14	<input type="checkbox"/>		
15	<input type="checkbox"/>		
16	<input type="checkbox"/>		
17	<input type="checkbox"/>		
18	<input type="checkbox"/>		
19	<input type="checkbox"/>		
20	<input type="checkbox"/>		
21	<input type="checkbox"/>		
22	<input type="checkbox"/>		
23	<input type="checkbox"/>		
24	<input type="checkbox"/>		
25	<input type="checkbox"/>		
26	<input type="checkbox"/>		
27	<input type="checkbox"/>		
28	<input type="checkbox"/>		
29	<input type="checkbox"/>		
30	<input type="checkbox"/>		
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

Figure 7-13 WLAN : Local User Database

The following table describes the labels in this screen.

Table 7-10 WLAN : Local User Database

LABEL	DESCRIPTION
Active	Select this option to activate the user profile.

**Table 7-10 WLAN : Local User Database**

<b>LABEL</b>	<b>DESCRIPTION</b>
User Name	Enter the username (up to 31 characters) for this user profile.
Password	Type a password (up to 31 characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.17 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- **Authentication**  
Determines the identity of the users.
- **Accounting**  
Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your HomeSafe acts as a message relay between the wireless station and the network RADIUS server.

### Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**  
Sent by an access point requesting authentication.
- **Access-Reject**  
Sent by a RADIUS server rejecting access.
- **Access-Accept**  
Sent by a RADIUS server allowing access.
- **Access-Challenge**  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**  
Sent by the access point requesting accounting.
- **Accounting-Response**  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the wired network from unauthorized access.

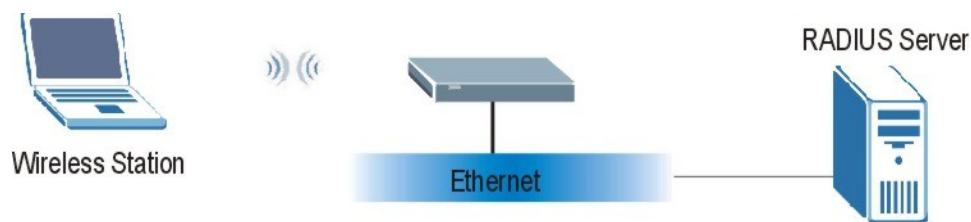
### 7.17.1 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The HomeSafe supports EAP-TLS, EAP-TTLS and DEAP with RADIUS. Refer to the *Types of EAP Authentication* appendix for descriptions on the four common types.

Your HomeSafe supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database and RADIUS.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.



**Figure 7-14 EAP Authentication**

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

- The wireless station sends a “start” message to the HomeSafe.
- The HomeSafe sends a “request identity” message to the wireless station for identity information.
- The wireless station replies with identity information, including username and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

## 7.18 Configuring RADIUS

Configure the RADIUS screen if you want to authenticate wireless users using an external server.

To specify a RADIUS server, click the **WIRELESS** link under **ADVANCED** and then the **RADIUS** tab. The screen appears as shown.

**WIRELESS LAN**

Wireless    MAC Filter    Roaming    Local User Database    **RADIUS**

**Authentication Server**

Active: No  
 Server IP Address: 0.0.0.0  
 Port Number: 1812  
 Shared Secret:

**Accounting Server**

Active: No  
 Server IP Address: 0.0.0.0  
 Port Number: 1813  
 Shared Secret:

Apply    Reset

Figure 7-15 WLAN : RADIUS

The following table describes the labels in this screen.

Table 7-11 WLAN : RADIUS

LABEL	DESCRIPTION
<b>Authentication Server</b>	
Active	Select <b>Yes</b> from the drop down list box to enable user authentication through an external authentication server.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the HomeSafe. The key must be the same on the external authentication server and your HomeSafe. The key is not sent over the network.
<b>Accounting Server</b>	
Active	Select <b>Yes</b> from the drop down list box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the HomeSafe. The key must be the same on the external accounting server and your HomeSafe. The key is not sent over the network.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.

**Table 7-11 WLAN : RADIUS**

LABEL	DESCRIPTION
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.





# Chapter 8

## WAN Screens

*This chapter describes how to configure WAN settings.*

### 8.1 WAN Overview

See the *Wizard Setup* chapter for more information on the fields in the WAN screens.

### 8.2 TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the HomeSafe's routes to the Internet. If the routes have the same metric, the HomeSafe uses the following pre-defined priorities:

1. **WAN**: designated by the ISP (see *Section 8.5*) or a static route (see the IP Static Route Setup chapter)
2. **Traffic Redirect** (see *Section 8.8*)

For example, if **WAN** has a metric of "1" and **Traffic Redirect** has a metric of "2", the **WAN** connection acts as the primary default route. If the **WAN** route fails to connect to the Internet, the HomeSafe tries **Traffic Redirect** next.

### 8.3 Configuring Route

Click **WAN** to open the **Route** screen.

**WAN**

Route | WAN ISP | WAN IP | WAN MAC | Traffic Redirect

**Route Selection**

WAN	Priority (metric)	1	Priority = 1(highest)-15(lowest)
Traffic Redirect	Priority (metric)	14	Priority = 1(highest)-15(lowest)

Apply Reset

**Figure 8-1 WAN : Route**

The following table describes the labels in this screen.

Table 8-1 WAN : Route

LABEL	DESCRIPTION
WAN Traffic Redirect	The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is <b>WAN</b> and then <b>Traffic Redirect</b> .
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.4 Configuring WAN ISP

To change your HomeSafe's WAN ISP settings, click **WAN**, then the **WAN ISP** tab. The screen differs by the encapsulation.

### 8.4.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

The screenshot shows the 'WAN' configuration interface. At the top, there are five tabs: 'Route', 'WAN ISP' (which is highlighted in yellow), 'WAN IP', 'WAN MAC', and 'Traffic Redirect'. Below the tabs, the 'WAN ISP' section is titled 'ISP Parameters for Internet Access'. It contains several input fields: 'Encapsulation' is a dropdown menu set to 'Ethernet'; 'Service Type' is a dropdown menu set to 'RR-Toshiba'; 'User Name' is a text input field; 'Password' and 'Retype to Confirm' are password input fields, both showing asterisks; and 'Login Server IP Address' is a text input field set to '0.0.0.0'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Figure 8-2 WAN ISP : Ethernet Encapsulation

The following table describes the labels in this screen.

Table 8-2 WAN ISP : Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from <b>Standard</b> , <b>Telstra</b> (RoadRunner Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method), <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method) or <b>Telia Login</b> . The following fields do not appear with the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type the password again to make sure that you have entered it correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.

**Table 8-2 WAN ISP : Ethernet Encapsulation**

<b>LABEL</b>	<b>DESCRIPTION</b>
Login Server	This field only applies when you select <b>Telia Login</b> in the <b>Service Type</b> field. Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Every(min)	This field only applies when you select <b>Telia Login</b> in the <b>Service Type</b> field. The Telia server logs the HomeSafe out if the HomeSafe does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the HomeSafe to wait between logins.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 8.4.2 PPPoE Encapsulation

The HomeSafe supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the HomeSafe (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the HomeSafe does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

**WAN**

Route | **WAN ISP** | WAN IP | WAN MAC | Traffic Redirect

**ISP Parameters for Internet Access**

Encapsulation: PPP over Ethernet

Service Name: (Optional)

User Name:

Password:

Retype to Confirm:

☐ Nailed-Up Connection

Idle Timeout: 100 (Seconds)

Apply Reset

Figure 8-3 WAN ISP : PPPoE Encapsulation

The following table describes the labels in this screen.

Table 8-3 WAN ISP : PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The <b>PPP over Ethernet</b> choice is for a dial-up connection using PPPoE. The HomeSafe supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 8.4.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

The screen shown next is for **PPTP** encapsulation.

**Figure 8-4 WAN ISP : PPTP Encapsulation**

The following table describes the labels in this screen.

**Table 8-4 WAN ISP : PPTP Encapsulation**

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The HomeSafe supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the HomeSafe automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.

**Table 8-4 WAN ISP : PPTP Encapsulation**

LABEL	DESCRIPTION
My IP Subnet Mask	Your HomeSafe will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the HomeSafe.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.5 Configuring WAN IP

To change your HomeSafe's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**; otherwise click **Use fixed IP Address** and enter the IP address in the field provided.

**WAN**

Route   WAN ISP   **WAN IP**   WAN MAC   Traffic Redirect

**WAN IP Address Assignment**

☒ Get automatically from ISP (Default)  
☐ Use fixed IP address

My WAN IP Address: 0.0.0.0  
 My WAN IP Subnet Mask: 0.0.0.0  
 Gateway IP Address: 0.0.0.0

Network Address Translation: SUA Only  
 RIP Direction: None  
 RIP Version: RIP-1  
 Multicast: IGMP-v1

**Windows Networking (NetBIOS over TCP/IP)**

☐ Allow between LAN and WAN (You also need to create a firewall rule)  
☐ Allow Trigger Dial

Apply   Reset

**Figure 8-5 WAN : IP**

The following table describes the labels in this screen.

**Table 8-5 WAN : IP**

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.

Table 8-5 WAN : IP

LABEL	DESCRIPTION
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
My WAN IP Subnet Mask (Ethernet only)	Type your network's IP subnet Mask.
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Gateway/Remote IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose <b>None</b> to disable NAT.</p> <p>Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b>.</p> <p>Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b>, <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b>, <b>Many- One-to-One</b> and <b>Server</b>. When you select <b>Full Feature</b> you must configure at least one address mapping set!</p> <p>For more information about NAT refer to the <i>NAT</i> chapter in this <i>User's Guide</i>.</p>
Metric (PPPoE and PPTP only)	<p>This field sets this route's priority among the routes the HomeSafe uses.</p> <p>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".</p>
Private (PPPoE and PPTP only)	This parameter determines if the HomeSafe will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the HomeSafe will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the HomeSafe will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the HomeSafe will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>



Table 8-5 WAN : IP

LABEL	DESCRIPTION
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the HomeSafe sends (it recognizes both formats when receiving). Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Multicast	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.</p>
<p>Windows Networking (NetBIOS over TCP/IP):</p> <p>NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.</p>	
Allow between WAN and LAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.6 Configuring WAN MAC

To change your HomeSafe's WAN MAC settings, click **WAN**, then the **WAN MAC** tab. The screen appears as shown.

Figure 8-6 WAN : MAC Setup

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

## 8.7 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the HomeSafe cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the HomeSafe still provides firewall protection.

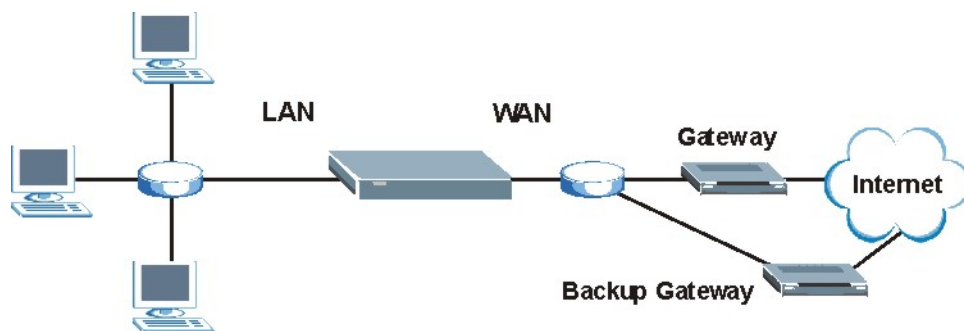


Figure 8-7 Traffic Redirect WAN Setup

The following network topology allows you to avoid triangle route security issues (see the *Appendices*) when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the HomeSafe itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/HomeSafe firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

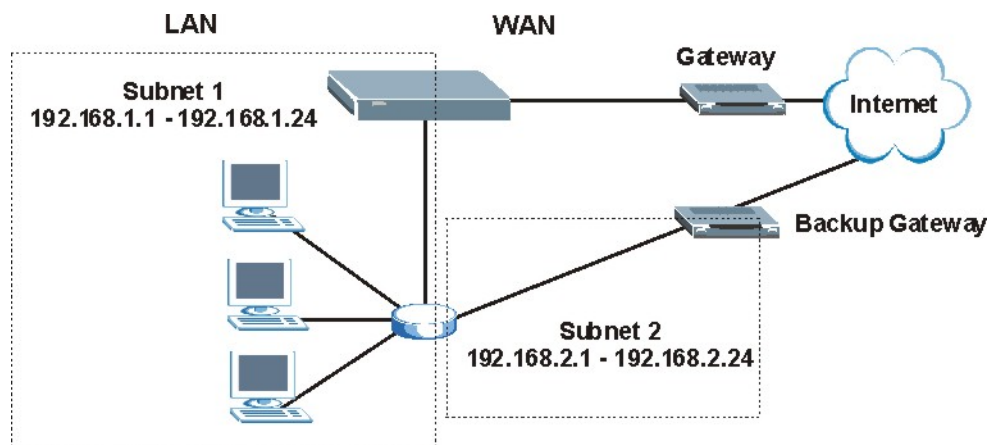


Figure 8-8 Traffic Redirect LAN Setup

## 8.8 Configuring Traffic Redirect

To change your HomeSafe's Traffic Redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown.

**Figure 8-9 WAN : Traffic Redirect**

The following table describes the labels in this screen.

**Table 8-6 WAN : Traffic Redirect**

LABEL	DESCRIPTION
Active	Select this check box to have the HomeSafe use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The HomeSafe automatically forwards traffic to this IP address if the HomeSafe's Internet connection terminates.
Metric	This field sets this route's priority among the routes the HomeSafe uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the HomeSafe will use the default gateway IP address. Configure this field to test your HomeSafe's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the HomeSafe to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your HomeSafe may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (seconds)	Type the number of seconds for the HomeSafe to wait between checks to see if it can connect to the WAN IP address ( <b>Check WAN IP Address</b> field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (seconds)	Type the number of seconds for your HomeSafe to wait for a ping response from the IP Address in the <b>Check WAN IP Address</b> field before it times out. The WAN connection is considered "down" after the HomeSafe times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.

**Table 8-6 WAN : Traffic Redirect**

<b>LABEL</b>	<b>DESCRIPTION</b>
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

---

---

## Part III:

---

### SUA/NAT and Static Route

---

This part covers Network Address Translation and setting up static routes.



# Chapter 9

## Network Address Translation (NAT)

### Screens

*This chapter discusses how to configure NAT on the HomeSafe.*

#### 9.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

##### 9.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the HomeSafe. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 9-1 NAT Definitions**

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.



**NAT never changes the IP address (either local or global) of an outside host.**

##### 9.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. If you do not define any servers

(for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your HomeSafe filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

### 9.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The HomeSafe keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

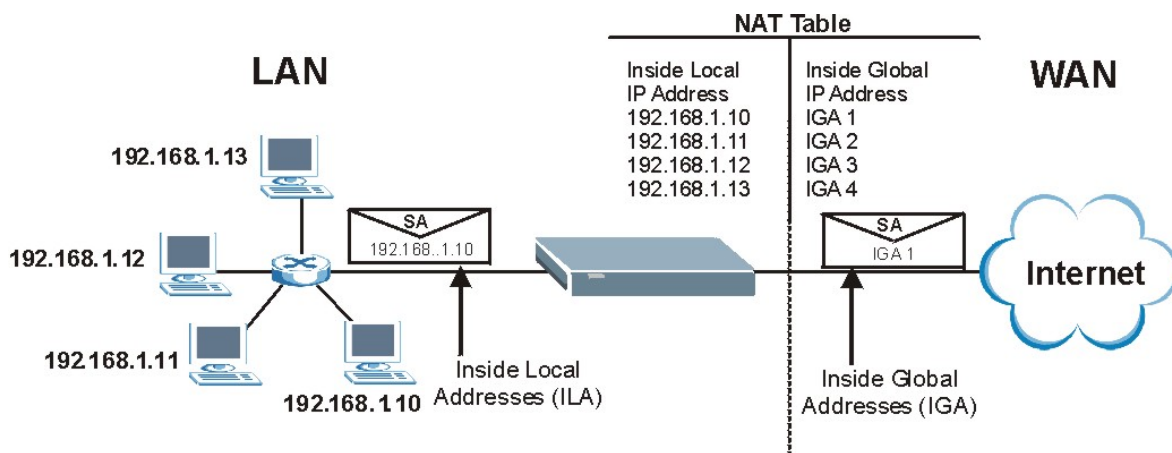


Figure 9-1 How NAT Works

### 9.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the HomeSafe can communicate with three distinct WAN networks. More examples follow at the end of this chapter.



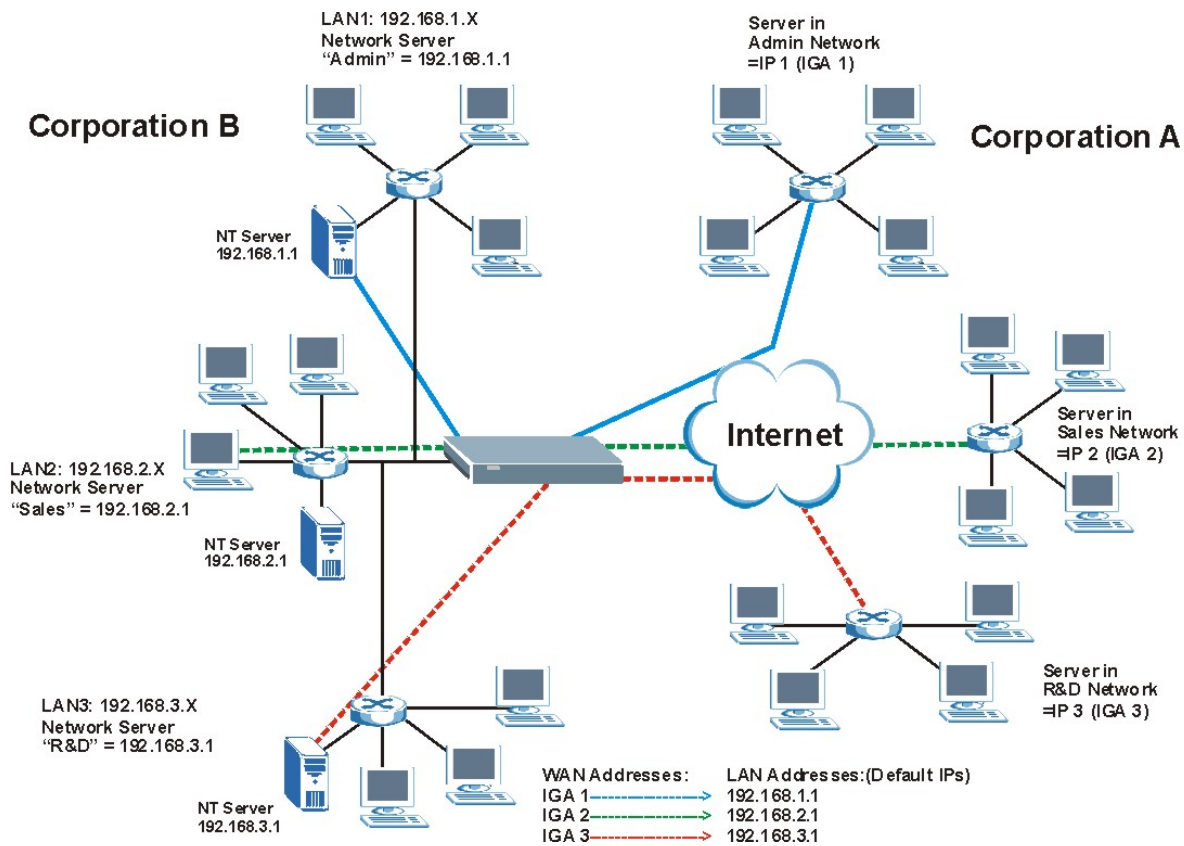


Figure 9-2 NAT Application With IP Alias

### 9.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the HomeSafe maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the HomeSafe maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **Many-to-Many Overload:** In Many-to-Many Overload mode, the HomeSafe maps the multiple local IP addresses to shared global IP addresses.
- **Many One-to-One:** In Many-One-to-One mode, the HomeSafe maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.



**Port numbers do not change for One-to-One and Many One-to-One NAT mapping types.**

The following table summarizes these types.

**Table 9-2 NAT Mapping Types**

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1↔IGA1	1-1
Many-to-One (SUA/PAT)	ILA1↔IGA1 ILA2↔IGA1 ...	M-1
Many-to-Many Overload	ILA1↔IGA1 ILA2↔IGA2 ILA3↔IGA1 ILA4↔IGA2 ...	M-M Ov
Many One-to-One	ILA1↔IGA1 ILA2↔IGA2 ILA3↔IGA3 ...	M-1-1
Server	Server 1 IP↔IGA1 Server 2 IP↔IGA1 Server 3 IP↔IGA1	Server

## 9.2 Using NAT



**You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the HomeSafe.**

### 9.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The HomeSafe also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in the **WAN IP** screen.

## 9.3 SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

## Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.



**If you do not assign a Default Server IP Address, the HomeSafe discards all packets received for ports that are not specified in this screen or remote management.**

### 9.3.1 Port Forwarding: Services and Port Numbers

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **SUA Server** page to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.



**Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.**

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

**Table 9-3 Services and Port Numbers**

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

### 9.3.2 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

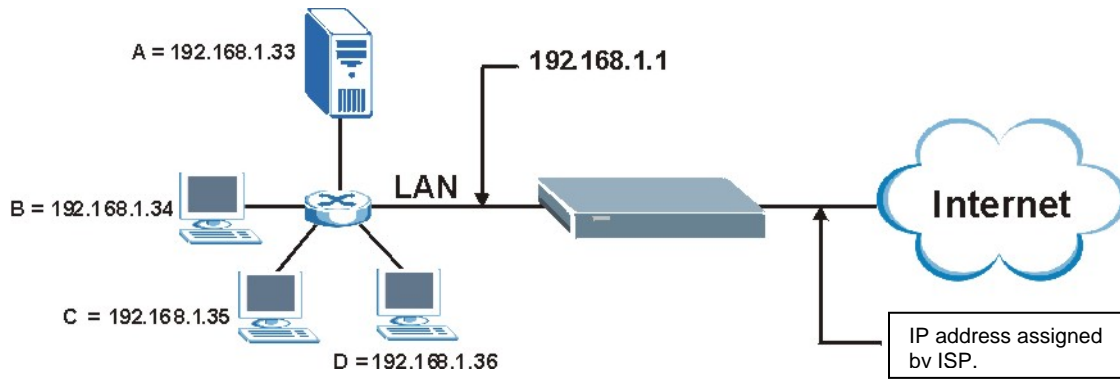


Figure 9-3 Multiple Servers Behind NAT Example

## 9.4 Configuring SUA Server



**If you do not assign a Default Server IP Address, the HomeSafe discards all packets received for ports that are not specified in this screen or remote management.**

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to *Table 9-3* for port numbers commonly used for particular services.

**SUA/NAT**

SUA Server    Addr Mapping    Trigger Port

Default Server: 0.0.0.0

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0

Apply    Reset

Figure 9-4 SUA/NAT Setup

The following table describes the labels in this screen.

Table 9-4 SUA/NAT Setup

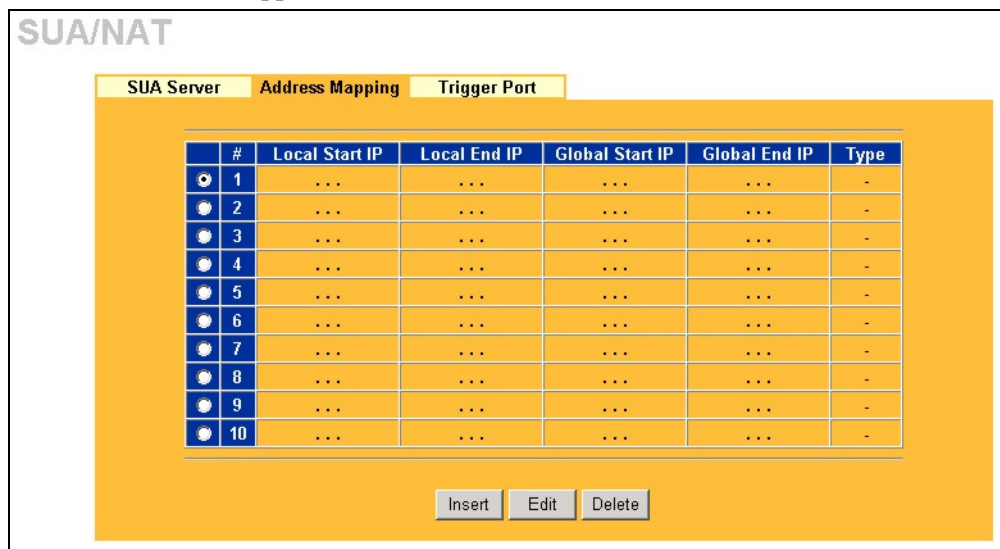
LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <b>Default Server</b> IP Address, the HomeSafe discards all packets received for ports that are not specified in this screen or remote management.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the <b>End Port</b> field. To specify a range of ports, enter the last port to be forwarded in the <b>End Port</b> field.
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 9.5 Configuring Address Mapping

Ordering your rules is important because the HomeSafe applies the rules in the order that you specify. When a rule matches the current packet, the HomeSafe takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the

set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your HomeSafe's Address Mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.



**Figure 9-5 Address Mapping**

The following table describes the labels in this screen.

**Table 9-5 Address Mapping**

LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the <b>Local Start IP</b> address. Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the end Inside Global Address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Type	<ol style="list-style-type: none"> <li>1. <b>One-to-One</b> mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</li> <li>2. <b>Many-to-One</b> mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</li> <li>3. <b>Many-to-Many Overload</b> mode maps multiple local IP addresses to shared global IP addresses.</li> <li>4. <b>Many One-to-One</b> mode maps each local IP address to unique global IP addresses.</li> <li>5. <b>Server</b> allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li> </ol>
Insert	Click <b>Insert</b> to insert a new mapping rule before an existing one.
Edit	Click <b>Edit</b> to go to the <b>Address Mapping Rule</b> screen.
Delete	Click <b>Delete</b> to delete an address mapping rule.

## Configuring Address Mapping

To edit an address mapping rule, select the radio button of a rule and click the **Edit** button to display the screen shown next.

**Figure 9-6 Address Mapping Edit**

The following table describes the labels in this screen.

**Table 9-6 Address Mapping Edit**

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. <b>One-to-One</b> : One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. <b>Many-to-One</b> : Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. <b>Many-to-Many Overload</b> : Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. <b>Many One-to-One</b> : Many One-to-one mode maps each local IP address to unique global IP addresses. 5. <b>Server</b> : This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Cancel	Click <b>Cancel</b> to return to the previous screen and not save your changes.

## 9.6 Trigger Port Forwarding

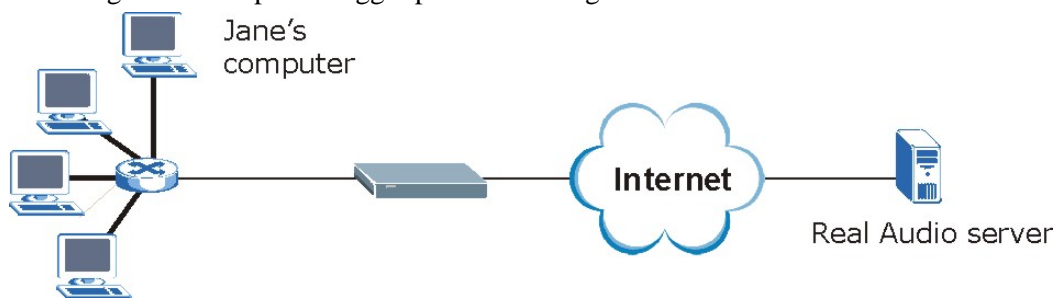
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a



service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address, Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The HomeSafe records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the HomeSafe's WAN port receives a response with a specific port number and protocol ("incoming" port), the HomeSafe forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

### 9.6.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.



**Figure 9-7 Trigger Port Forwarding Process: Example**

1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the HomeSafe to record Jane's computer IP address. The HomeSafe associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The HomeSafe forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The HomeSafe times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

### 9.6.2 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the HomeSafe and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

## 9.7 Configuring Trigger Port Forwarding

To change your HomeSafe's trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.





**Only one LAN computer can use a trigger port (range) at a time.**

SUA/NAT

SUA Server   Addr Mapping   **Trigger Port**

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

Apply   Reset

**Figure 9-8 Trigger Port**

The following table describes the labels in this screen.

**Table 9-7 Trigger Port**

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The HomeSafe forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the HomeSafe to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# Chapter 10

## Static Route Screens

*This chapter shows you how to configure static routes for your HomeSafe.*

### 10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the HomeSafe has no knowledge of the networks beyond. For instance, the HomeSafe knows about network N2 in the following figure through remote node router R1. However, the HomeSafe is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node router R1 (via gateway router R2). The static routes are for you to tell the HomeSafe about the networks beyond the remote nodes.

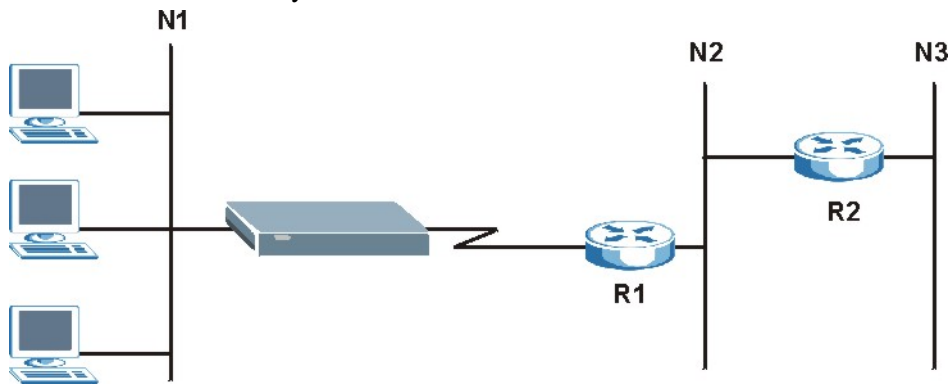


Figure 10-1 Example of Static Routing Topology

### 10.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the screen as shown next.

STATIC ROUTE

IP Static Route

	#	Name	Active	Destination	Gateway
	1	-	-	...	...
	2	-	-	...	...
	3	-	-	...	...
	4	-	-	...	...
	5	-	-	...	...
	6	-	-	...	...
	7	-	-	...	...
	8	-	-	...	...

Edit Delete

Figure 10-2 Static Route

The following table describes the labels in this screen.

**Table 10-1 Static Route**

LABEL	DESCRIPTION
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your HomeSafe that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your HomeSafe; over the WAN, the gateway must be the IP address of one of the remote nodes.
Edit	Select a static route index number and then click <b>Edit</b> to set up a static route on the HomeSafe.

### 10.2.1 Configuring Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

**STATIC ROUTE - EDIT**

Route Name

☐ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

☐ Private

**Figure 10-3 Static Route: Edit**

The following table describes the labels in this screen.

**Table 10-2 Static Route: Edit**

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your HomeSafe that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your HomeSafe; over the WAN, the gateway must be the IP address of one of the Remote Nodes.

**Table 10-2 Static Route: Edit**

<b>LABEL</b>	<b>DESCRIPTION</b>
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the HomeSafe will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Cancel	Click <b>Cancel</b> to return to the previous screen and not save your changes.

---

## Part IV:

---

### UPnP, Parental Control and Firewall

---

This part provides information and configuration instructions for configuration of Universal Plug and Play, parental control, firewall and content filtering.

# Chapter 11

## UPnP

*This chapter introduces the Universal Plug and Play feature.*

### 11.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

#### 11.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### 11.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the *SUA/NAT* chapter for further information about NAT.

#### 11.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

### 11.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet

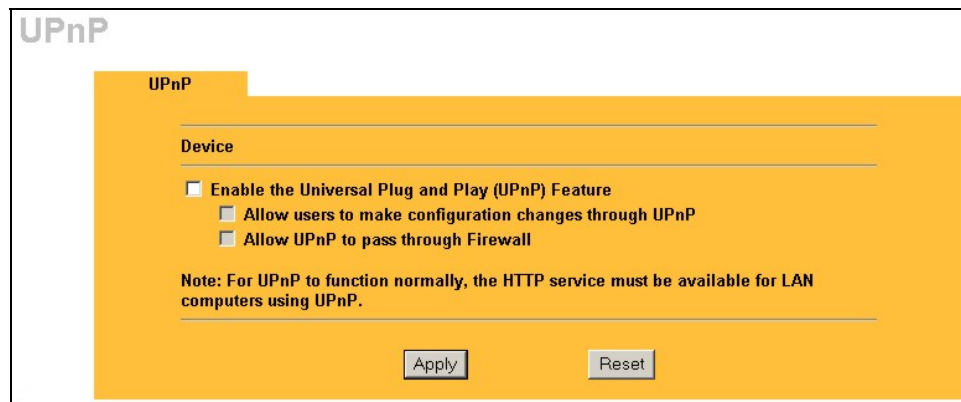
Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

UPnP broadcasts are only allowed on the LAN.

Please see later in this *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

## 11.3 Configuring UPnP

Click **UPnP** to display the screen shown next.



**Figure 11-1 Configuring UPnP**

The following table describes the labels in this screen.

**Table 11-1 Configuring UPnP**

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the HomeSafe's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the HomeSafe so that they can communicate through the HomeSafe, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 11.4 Installing UPnP in Windows Example

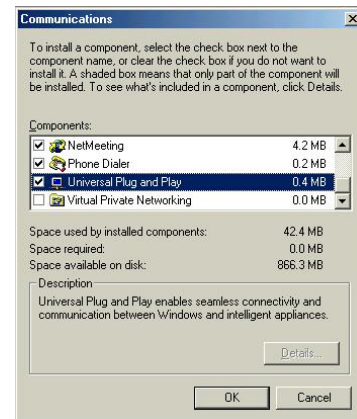
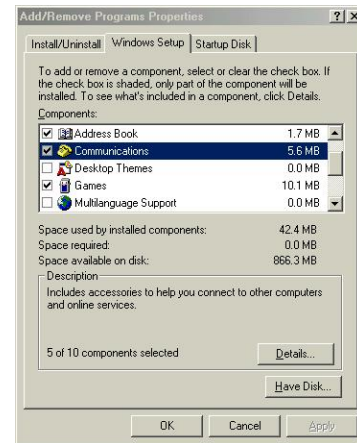
This section shows how to install UPnP in Windows Me and Windows XP.



### 11.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

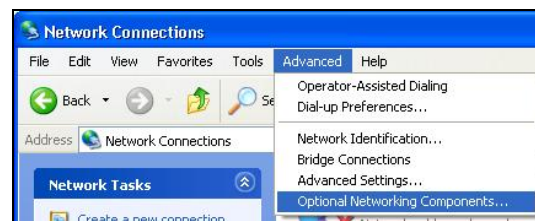
- Step 1.** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- Step 2.** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.
- Step 3.** In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- Step 4.** Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- Step 5.** Restart the computer when prompted.



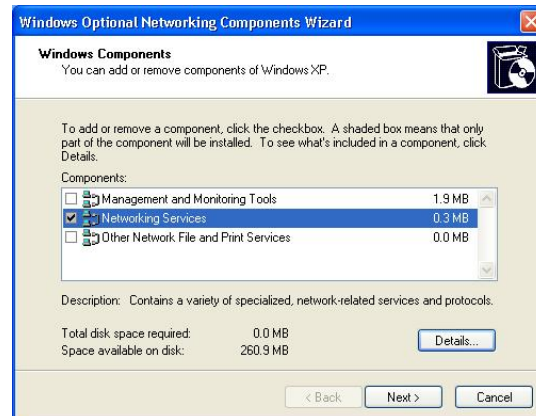
### 11.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

- Step 1.** Click **Start** and **Control Panel**.
- Step 2.** Double-click **Network Connections**.
- Step 3.** In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**. The **Windows Optional Networking Components Wizard** window displays.

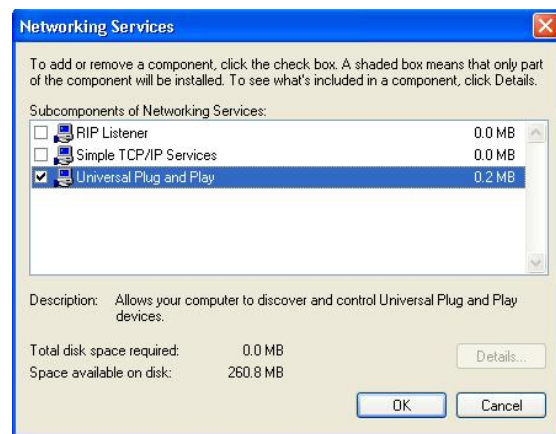


- Step 4.** Select **Networking Service** in the **Components** selection box and click **Details**.



- Step 5.** In the **Networking Services** window, select the **Universal Plug and Play** check box.

- Step 6.** Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



## 11.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

### 11.5.1 Auto-discover Your UPnP-enabled Network Device

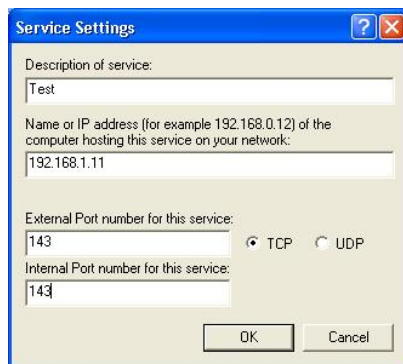
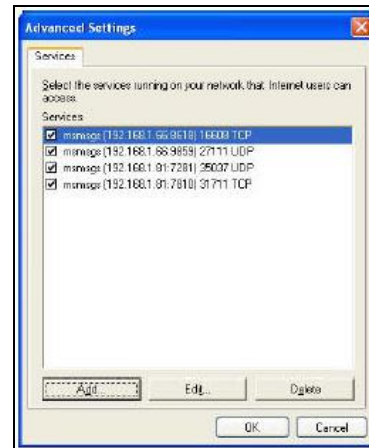
- Step 1.** Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- Step 2.** Right-click the icon and select **Properties**.



**Step 3.** In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

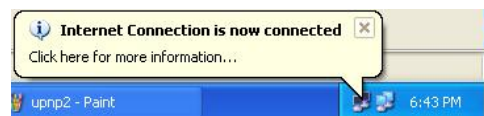


**Step 4.** You may edit or delete the port mappings or click **Add** to manually add port mappings.



**When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.**

**Step 5.** Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



- Step 6.** Double-click the icon to display your current Internet connection status.

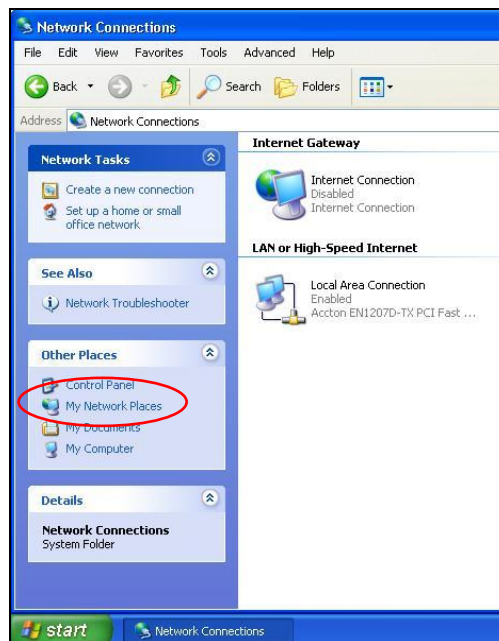


### 11.5.2 Web Configurator Easy Access

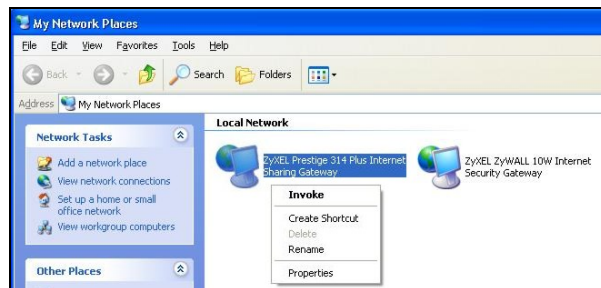
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

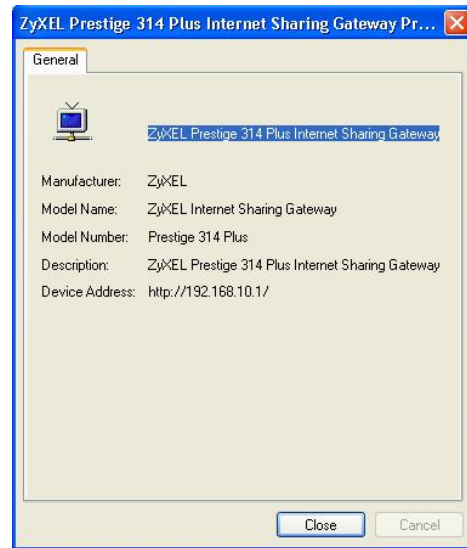
- Step 1.** Click Start and then Control Panel.
- Step 2.** Double-click **Network Connections**.
- Step 3.** Select **My Network Places** under **Other Places**.



- Step 4.** An icon with the description for each UPnP-enabled device displays under **Local Network**.
- Step 5.** Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.



- Step 6.** Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.





# Chapter 12

## Parental Control

*This chapter gives some background information on parental control and explains how to get started with the HomeSafe parental control.*

### 12.1 Parental Control Overview

Parental Control lets a parent (LAN administrator) control a child's (LAN user) Internet access privileges by blocking services that you specify. The parent can create a login name and password for each person (user) on the network. Each person must log into the system before they can gain access to the Internet.

### 12.2 Parental Control Logins

#### Initial Configuration

1. For initial configuration, the HomeSafe directs the browser to the HomeSafe Welcome page.
2. On completion of the initial configuration you can enter the Main Menu HomeSafe configuration screen or set up your computer to access the Internet. A password is required for both.

#### Child (User) log in

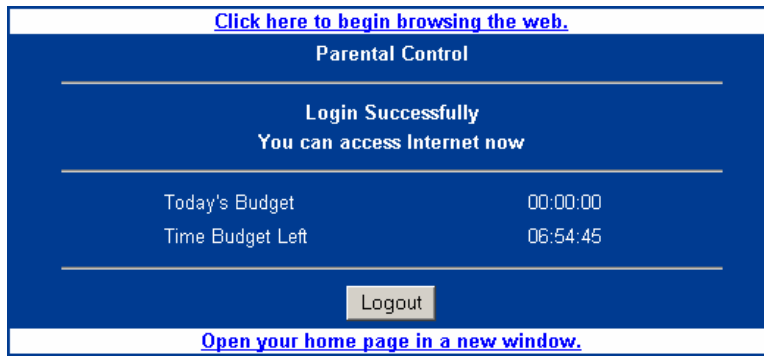
Once the initial configuration is complete, a computer on the network cannot gain Internet access without first logging into the HomeSafe.

1. When you attempt to access a website, you are directed to the HomeSafe's User Login page.



**Figure 12-1 HomeSafe Network User Login**

2. After you enter your login name and password the device checks the access profile and begins enforcing the access control restriction as defined by the administrator. The access privileges remain in force until you log out.
3. After a successful login, your web browser displays a window that shows the remaining budget time and a logout button.



**Figure 12-2 User Status Window**

4. You can start browsing the web from the current window, or use the link on the top of the box to open a new web browser.
  - If you close or navigate away from the status screen, you can redisplay the status screen by typing **status** into the address bar on your web browser and hitting enter.
5. There are five ways to be logged out of the system.
  - Click the Logout button on the status screen.
  - The idle timeout triggers the logout (the default is five minutes).
  - The access **Time Allowance** budget reaches zero and triggers the logout.
  - The system clock reaches the **End Time** for the user's account and triggers the logout.
  - Type **logout** into the address bar on your web browser and hitting enter.
- 6.

### **Parental (Administrator) log in**

The administrator can log into the system after the initial configuration.

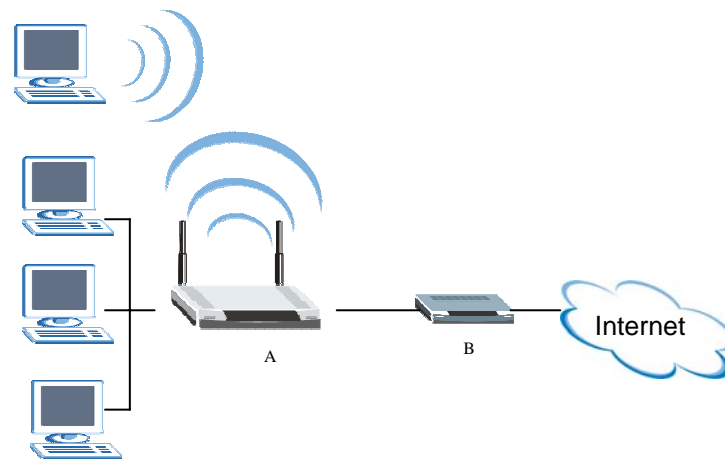
1. The administrator opens their browser and is directed to the HomeSafe User Login page (this is the same as the user login).
2. The administrator enters "admin" as the username and the system password.
3. The system administrator Welcome page opens.

## **12.3 Parental Control Application**

You can control LAN user Internet access by having an administrator configure parental control on the HomeSafe.

The parent (administrator) must create login names and passwords for each person (user) on the network. Each person must log into the system before they can gain access to the Internet. Each person's account will hold the details of their access rights and privileges. The HomeSafe enforces these access restrictions. In the following diagram, A refers to the HomeSafe and B refers to a modem.





**Figure 12-3 HomeSafe Parental Control Wireless Gateway Application**

## **12.4 Configuring Parental Control**

From the **MAIN MENU**, click **PARENTAL CONTROL** to open the configuration screen.

## Parental Control

General

Bypass List

Use the check box below to Enable/Disable the Parental Control Mode:

☒ **Enable Parental Control**

Idle user sessions will be automatically logged out of the parental control system if no Internet traffic is detected during the idle timeout period set below:

Idle Timeout  min

Use the "Group" pull down box to select a content filtering group and click "Edit" to view or change the current Web page categories settings for each group. Click the "Diagnose" to test a particular web page against the content filtering database.

Group

Click the "Register" button to register and subscribe this unit for content filtering service. Click the "Activate" button to activate a previously active subscription.

Content Filtering Service **Registered**

Use the +/- buttons under the Allowance Left column to quickly add or subtract time from today's remaining time allowance:

	Username	Group	Time Left	On-Line
<input type="button" value="⊕"/>	1	Adult	10:00 <input type="button" value="⊕"/> <input type="button" value="⊖"/>	Ready
<input type="button" value="⊕"/>	2	Kids	Unrestricted	Ready
<input type="button" value="⊕"/>				
<input type="button" value="⊕"/>				
<input type="button" value="⊕"/>				
<input type="button" value="⊕"/>				
<input type="button" value="⊕"/>				
<input type="button" value="⊕"/>				
<input type="button" value="⊕"/>				

Figure 12-4 Parental Control

The following table describes the labels in this screen.

Table 12-1 Parental Control

LABEL	DESCRIPTION
Enable Parental Control	Select the check box to allow the parent (LAN administrator) to have control over a child's (LAN user's) Internet access.
Idle Timeout	Type the time in minutes that elapses before the connection automatically terminates the Internet session. The default time is 5 minutes.

Table 12-1 Parental Control


LABEL	DESCRIPTION
Group	<p>Select from the drop-down list box a category of web pages that you want to have access control over</p> <ul style="list-style-type: none"> <li>➤ Kids</li> <li>➤ Young Teen</li> <li>➤ Mature Teen</li> <li>➤ Adult</li> </ul> <p>These groups are used in conjunction with content filtering to decide which web pages cannot be accessed by the user.</p>
Edit	Click <b>Edit</b> to proceed to a pre-defined web content categories page for the group that you select. Refer to <i>section 12.6</i> for more information.
Content Filtering Service	<p>The read only field Content Filtering Service Status displays <b>Not Registered</b> if you have not successfully registered the HomeSafe or your registration has expired.</p> <p>This field only displays whether or not you have successfully registered, not whether or not content filtering is active. See <i>Checking Content Filtering Activation</i> for details on how to check for this. Click <b>Register Now</b> to go to a web site where you can register for category-based content filtering (using an external database). You can use a trial application or register your iCard's PIN. Refer to the web site's on-line help for details.</p> <hr/> <div style="text-align: center;">  <p><b>The web site displays a registration successful web page. It may take up to another ten minutes for content filtering to be activated. See <i>Checking Content Filtering Activation</i> on how to check the content filtering activation.</b></p> </div> <hr/> <p>You can manage your registration status or view content filtering reports after you register this device.</p> <p>Click <b>Activate</b> to begin the content filtering service now.</p>
Username	This field displays the username (up to 30 characters) for this user profile.
Group	This field displays the name of the user group.
Time Left	This field displays the amount of time that you have before the HomeSafe logs you out and terminates your internet access. This time depends on the time allowance configured in <i>Figure 12-7</i> . By using the + or – buttons, the administrator can increase or decrease the time left in 15 minute increments without re-configuring the time allowances.
On-Line	<p>This field displays <b>Yes</b> if a user is currently on-line.</p> <p>This field displays <b>Ready</b> if a user has a profile configured with unrestricted access and is currently not on-line.</p> <p>This field displays <b>No</b> if a user has a profile configured with time allowances and is currently not on-line.</p>
Edit	Select a radio button from the list of profiles and then click <b>Edit</b> to configure this profile.
Delete	Select a radio button from the list of profiles and then click <b>Delete</b> to remove this profile from the list.
Apply	Click <b>Apply</b> to save the settings.

Table 12-1 Parental Control

LABEL	DESCRIPTION
Reset	Click <b>Reset</b> to start configuring this screen again.

## 12.5 Parental Control Group Edit Filter

The HomeSafe content filtering allows you to block services and block web sites by URL keywords that you specify, for example, you can block access to all web sites with the word “bad” in the URL by specifying “bad” as a keyword.

### 12.5.1 Content Filtering with an External Server

Your HomeSafe uses an application services company that provides outsourced content filtering. If you enable the content filter, your HomeSafe will have access to an external database, which contains dynamically updated ratings of millions of web sites.

The content filtering lookup process is described below.

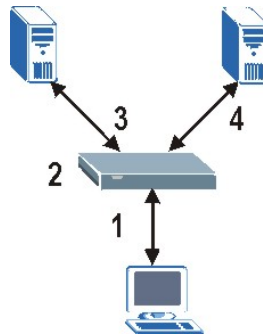


Figure 12-5 Content Filtering Lookup Procedure

1. A computer sends an HTTP request to a web server.
2. The HomeSafe looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the HomeSafe's cache. The HomeSafe either blocks or forwards the request based on how you configure the category based content filtering.

The HomeSafe drops a URL record from the content filter cache after the content filter cache timeout period (default 72 hours). All of the URL records are also cleared from the local cache when the HomeSafe reboots. You can use `ip urlfilter webControl cache timeout` on the command line to change the timeout period.

If the HomeSafe doesn't have a record of the web site, it will query the external content filtering server and simultaneously send the request to the web server.

The external content filtering database may change a web site's category or rate a previously uncategorized web site.

3. The external content filtering server sends the category information back to the HomeSafe, which then either forwards or blocks the web content. The web site address is then also stored in the HomeSafe's content filtering cache.

Pre-defined categories have a filtering process based on ports and services.

1. A computer sends service-based request.
2. The HomeSafe looks up the port that this service uses.

3. The HomeSafe either blocks or forwards the request based on the services you select in the **Available Services** field in the **Parental Control Activation Blocking** screen.

### Checking Content Filtering Activation

After you register for content filtering, the browser displays a registration successful web page. This does not mean the content filtering is active yet. You need to wait up to ten minutes for the content filtering to be activated.

Since there will be no activation notice, when content filtering is active, you should see an access blocked message when your HomeSafe has been setup with parental control and you try to access a restricted website or service.

## 12.6 Parental Control Group Edit Configuration

Select a group name and click **Edit** in the **Group** section of the **Parental Control** screen to proceed to a pre-defined web content categories page for the group selected.

The following table shows the default blocked Web page categories for each user group. The adult user group by default has no blocked Web pages.

TABLE 12-2 DEFAULT BLOCKED WEB CATEGORIES			
WEB PAGE CATEGORY	KIDS	YOUNG TEEN	MATURE TEEN
Abortion	X	X	
Adult/Mature	X	X	
Alcohol/ Tobacco	X	X	X
Cult/Occult	X	X	X
Gambling	X	X	X
Hacking/Proxy Avoidance	X	X	X
Illegal Drugs	X	X	X
Illegal/ Questionable	X	X	X
Intimate Apparel/Swimsuit	X		
Nudity	X	X	
Personals/Dating	X	X	
Pornography	X	X	X
Sex Education	X		
Violence/Hate/Racism	X	X	X
Weapons	X	X	

The screen appears as shown next. Use this screen to enable content filtering, configure URL keyword blocking by entering, deleting and modifying keywords that you want to block.

**Parental Control - Kids**

---

**Pre-defined Web Content Categories**  
☒ **Enable**

**Select Blocked Categories**

<input checked="" type="checkbox"/> Abortion	<input checked="" type="checkbox"/> Adult/Mature Content	<input checked="" type="checkbox"/> Alcohol/Tobacco
<input type="checkbox"/> Arts/Entertainment	<input type="checkbox"/> Auctions	<input type="checkbox"/> Brokerage/Trading
<input type="checkbox"/> Business/Economy	<input type="checkbox"/> Chat/Instant Messaging	<input type="checkbox"/> Computers/Internet
<input checked="" type="checkbox"/> Cult/Occult	<input type="checkbox"/> Cultural Institutions	<input type="checkbox"/> Education
<input type="checkbox"/> Email	<input type="checkbox"/> Financial Services	<input type="checkbox"/> For Kids
<input checked="" type="checkbox"/> Gambling	<input type="checkbox"/> Games	<input type="checkbox"/> Gay/Lesbian
<input type="checkbox"/> Government/Legal	<input checked="" type="checkbox"/> Hacking/Proxy Avoidance	<input type="checkbox"/> Health
<input type="checkbox"/> Humor/Jokes	<input checked="" type="checkbox"/> Illegal Drugs	<input checked="" type="checkbox"/> Illegal/Questionable
<input checked="" type="checkbox"/> Intimate Apparel/Swimsuit	<input type="checkbox"/> Job Search/Careers	<input type="checkbox"/> Military
<input type="checkbox"/> News/Media	<input type="checkbox"/> Newsgroups	<input checked="" type="checkbox"/> Nudity
<input type="checkbox"/> Pay to Surf	<input checked="" type="checkbox"/> Personals/Dating	<input type="checkbox"/> Political/Activist Groups
<input checked="" type="checkbox"/> Pornography	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Reference
<input type="checkbox"/> Religion	<input type="checkbox"/> Restaurants/Dining/Food	<input type="checkbox"/> Search Engines/Portals
<input checked="" type="checkbox"/> Sex Education	<input type="checkbox"/> Shopping	<input type="checkbox"/> Society/Lifestyle
<input type="checkbox"/> Software Downloads	<input type="checkbox"/> Sports/Recreation/Hobbies	<input type="checkbox"/> Streaming Media/MP3
<input type="checkbox"/> Travel	<input type="checkbox"/> Unrated	<input type="checkbox"/> Vehicles
<input checked="" type="checkbox"/> Violence/Hate/Racism	<input checked="" type="checkbox"/> Weapons	<input type="checkbox"/> Web Advertisements
<input type="checkbox"/> Web Communications	<input type="checkbox"/> Web Hosting	

basic...

---

**Keyword Blocking**  
☐ **Enable**

Block Websites that contain these keywords in the URL:

**Keyword**

---

**Figure 12-6 Parental Control : Filter**

The following table describes the labels in this screen.

**Table 12-3 Parental Control : Filter**

LABEL	DESCRIPTION
Pre-defined Web Content Categories	Enable <b>Pre-defined Web Content Categories</b> to have the HomeSafe check an external database to find to which category a requested web page belongs. The HomeSafe then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Select Blocked Categories	Use this section to prevent users from accessing web pages that match the categories that you select below.
Select All	Select this check box to restrict access to all site categories listed below.
Clear All	Select this check box to clear the selected categories below.
Adult/Mature Content	Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children.
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.

**Table 12-3 Parental Control : Filter**

<b>LABEL</b>	<b>DESCRIPTION</b>
Sex Education	Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement.
Intimate Apparel/Swimsuit	Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered.
Nudity	Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals.
Alcohol/Tobacco	Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products.
Illegal/Questionable	Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers.
Gambling	Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements).
Violence/Hate/Racism	Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics.
Weapons	Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use.
Abortion	Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Arts/Entertainment	Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment.

**Table 12-3 Parental Control : Filter**

<b>LABEL</b>	<b>DESCRIPTION</b>
Business/Economy	Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services).
Cult/Occult	Selecting this category excludes pages that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers and satanic or supernatural beings.
Illegal Drugs	Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Education	Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups.
Cultural Institutions	Selecting this category excludes pages sponsored by cultural institutions, or those that provide information about museums, galleries, and theaters (not movie theaters). It includes groups such as 4H and the Boy Scouts of America.
Financial Services	Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services.
Brokerage/Trading	Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news.
Games	Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways.
Government/Legal	Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities.
Military	Selecting this category excludes pages that promote or provide information on military branches or armed services.
Political/Activist Groups	Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities.
Health	Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition.



**Table 12-3 Parental Control : Filter**

<b>LABEL</b>	<b>DESCRIPTION</b>
Computers/Internet	Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies.
Hacking/Proxy Avoidance	Pages providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.
Search Engines/Portals	Selecting this category excludes pages that support searching the Internet, indices, and directories.
Web Communications	Selecting this category excludes pages that allow or offer Web-based communication via e-mail, chat, instant messaging, message boards, etc.
Job Search/Careers	Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers.
News/Media	Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories.
Personals/Dating	Selecting this category excludes pages that promote interpersonal relationships.
Reference	Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information.
Chat/Instant Messaging	Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads.
Email	Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services.
Newsgroups	Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems.
Religion	Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups).
Shopping	Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons).
Auctions	Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements.
Real Estate	Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties.
Society/Lifestyle	Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category.

Table 12-3 Parental Control : Filter


LABEL	DESCRIPTION
Gay/Lesbian	Selecting this category excludes pages that provide information, promote, or cater to gay and lesbian lifestyles. This does not include pages that are sexually oriented.
Restaurants/Dining/Food	Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes.
Sports/Recreation/Hobbies	Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting.
Travel	Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
Vehicles	Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts.
Humor/Jokes	Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating.
Streaming Media/MP3	Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including pages that provide downloads for such viewers.
Software Downloads	Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge.
Pay to Surf	Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
For Kids	Selecting this category excludes pages designed specifically for children.
Web Advertisements	Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.
Web Hosting	Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services.
Advanced/Basic	Click <b>more...</b> to see an expanded list of categories, or click <b>basic...</b> to see a smaller list.
Keyword Blocking	<p>Select the Enable check box to block the URL containing the keywords in the keyword list.</p> <hr/> <p> <b>See the Customizing Keyword Blocking URL Checking section for how to set how much of the URL the HomeSafe checks.</b></p> <hr/>
Block Websites that contain these keywords in the URL	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Delete	Select a keyword from the keyword list and then click <b>Delete</b> to remove this keyword from the list.

Table 12-3 Parental Control : Filter

LABEL	DESCRIPTION
Clear All	Click <b>Clear All</b> to empty the keyword list.
Keyword	Type a keyword in the <b>Keyword</b> field and click then <b>Add Keyword</b> to add a keyword to the list of keywords. The list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Close	Click <b>Close</b> to exit this screen without saving changes.
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 12.7 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

### 12.7.1 Domain Name or IP Address URL Checking

By default, the HomeSafe checks the URL's domain name or IP address when performing keyword blocking.

This means that the HomeSafe checks the characters that come before the first slash in the URL.

For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), content filtering only searches for keywords within [www.zyxel.com.tw](http://www.zyxel.com.tw).

### 12.7.2 Full Path URL Checking

Full path URL checking has the HomeSafe check the characters that come before the last slash in the URL.

For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), full path URL checking searches for keywords within [www.zyxel.com.tw/news/](http://www.zyxel.com.tw/news/).

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

### 12.7.3 File Name URL Checking

Filename URL checking has the HomeSafe check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php).

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

## 12.8 Parental Control Edit

Select an account profile radio button in the **Parental Control** screen and click **Edit**.

### 12.8.1 Services

The **Available Services** list box in the **Edit Rule** screen displays some predefined services that the HomeSafe supports. The following table shows a list of services that can be configured. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol

type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. (UDP/TCP:53) means UDP port 53 and TCP port 53.

**Table 12-4 Services**

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.

**Table 12-4 Services**

<b>SERVICE</b>	<b>DESCRIPTION</b>
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

The following screen allows you to edit login information, configure time scheduling, choose what type of services you want to block and edit customized services.

## Parental Control

**Login Information:**

Username:

Password:

Group:

**Time Scheduling:**

☐ Allow  hr  min access from  to  everyday

☒ Allow Custom Daily Access

	Unrestricted	Budget Left	Start Time	End Time
Monday	<input type="checkbox"/>	3 hr 0 min	08:00AM	11:00AM
Tuesday	<input type="checkbox"/>	0 hr 0 min	Midnight	Midnight
Wednesday	<input type="checkbox"/>	0 hr 0 min	Midnight	Midnight
Thursday	<input type="checkbox"/>	0 hr 0 min	Midnight	Midnight
Friday	<input type="checkbox"/>	0 hr 0 min	Midnight	Midnight
Saturday	<input type="checkbox"/>	0 hr 0 min	Midnight	Midnight
Sunday	<input type="checkbox"/>	0 hr 0 min	Midnight	Midnight

**Service to be blocked:**

**Available Services:**

- Chat or Instant Messenger - ICQ (UDP:4000)
- Chat or Instant Messenger - IRC (TCP/UDP:6667)
- Chat or Instant Messenger - MSN Messenger (TCP:1863)
- Internet Telephone - CU-SEEME (TCP/UDP:7648,24032)
- Internet Telephone - H.323 (TCP:1720)
- Internet Telephone - VDOLIVE (TCP:7000)
- File Sharing - e-Donkey (TCP:4661 - 4662)
- File Transfers - FTP (TCP:20,21)
- Web Browsing - HTTP (TCP:80)
- Web Browsing - HTTPS (TCP:443)
- E-Mail - Receiving (TCP:110)
- E-Mail - Sending (TCP:25)
- Streaming Video and Audio - REAL-AUDIO (TCP:7070)

**Weekdays:**

- Chat or Instant Messenger - IRC (TCP/UDP:6667)
- Chat or Instant Messenger - MSN Messenger (TCP:1863)
- Internet Telephone - CU-SEEME (TCP/UDP:7648,24032)
- Chat or Instant Messenger - ICQ (UDP:4000)

**Weekend:**

- Streaming Video and Audio - REAL-AUDIO (TCP:7070)
- Games - StarCraft (TCP:6112)

**Edit Customized Services**

Type	Port Number
TCP	0 - 0

Figure 12-7 Parental Control : Edit

The following table describes the labels in this screen.

Table 12-5 Parental Control : Edit

LABEL	DESCRIPTION
Username	Type a name to identify this user.
Password	Type a password. This password is used each time you log in to access the Internet.

Table 12-5 Parental Control : Edit



LABEL	DESCRIPTION
Groups	<p>Select a group from the drop down list box. The category of web pages to block are grouped as one of the following</p> <ul style="list-style-type: none"> <li>➤ Kids</li> <li>➤ Young Teen</li> <li>➤ Mature Teen</li> <li>➤ Adult</li> </ul> <p>These groups are used in conjunction with content filtering to decide which web pages, cannot be accessed by the user.</p>
Time Scheduling	<p>Select the first radio button to allow everyday access at the same times to the Internet. Type the interval time allowance (number of hours and minutes). Select the start and end times from the drop-down list boxes to configure the period during the day when access is allowed.</p> <p>Select <b>Allow Custom Daily Access</b> to configure time allowances, start times and end times for each day.</p>
Unrestricted	<p>Select the check box for the day(s) that you do not want any time restrictions for user Internet access.</p>
Time Allowance (hr:min)	<p>Type the number of hours (0 to 23) and minutes (0 to 59) to allow Internet access of unblocked sites.</p> <hr/> <p> <b>If you want to allow twenty-four hour access, you should select the unrestricted check box.</b></p> <hr/>
Start Time	<p>Select from the drop-down list box a time during the day when a user can begin accessing unblocked sites.</p>
End Time	<p>Select from the drop-down list box a time during the day when a user can no longer access unblocked sites. The time allowance must be less than or equal to the period from the start time to the end time.</p> <hr/> <p> <b>User access will be denied after the End Time for that day even if the time allowance has not run out.</b></p> <hr/>
Service to be Blocked	
Available services	<p>Select a service from the list and click the &gt;&gt; button to have the service blocked on a weekday (Monday to Friday) or to have the service blocked on a day in the weekend (Saturday or Sunday).</p> <p>These services will be blocked according to the settings you configure in <b>Time Scheduling</b>.</p>
Weekdays	<p>This box shows all the services that you want to block on weekdays for the user group. Click the &lt;&lt; button to remove a service from the box.</p>
Weekend	<p>This box shows all the services that you want to block on weekends for the user group. Click the &lt;&lt; button to remove a service from the box.</p>

Table 12-5 Parental Control : Edit

LABEL	DESCRIPTION
Edit Customized Services	A <b>Customized Service</b> is a service that is not available in the pre-defined <b>Available Services</b> list and you must define using the next two fields.
Type	Services are either <b>TCP</b> and/or <b>UDP</b> . Select from either <b>TCP</b> or <b>UDP</b> .
Port Number	Enter a port number or a range of port numbers to define the service. For example, suppose you want to define the Gnutella service. Select <b>TCP</b> type and enter a port range from 6345-6349.
Add to Weekdays/ Add to Weekend	Click <b>Add to Weekdays</b> or <b>Add to Weekend</b> to add a service to be blocked to the <b>Weekdays</b> or <b>Weekend</b> boxes.
Clear All	Click <b>Clear All</b> to empty the <b>Weekdays</b> or <b>Weekend</b> boxes.
Back	Click <b>Back</b> to display the previous screen.
Apply	Click <b>Apply</b> to save the settings.
Reset	Click <b>Reset</b> to start configuring this screen again.

## 12.9 Parental Control Bypass List

Use this screen to allow a device on your LAN to bypass HomeSafe parental controls based on the MAC address of the device. You can configure up to ten users in this list to bypass parental controls. When the user accesses the Internet, the parental control login screen is not displayed.

The screenshot shows the 'Parental Control Bypass List' configuration screen. It features a table with 10 rows for adding devices to the bypass list. Each row contains a 'Name' field and a 'MAC Address' field. At the bottom of the screen, there are 'Apply' and 'Reset' buttons.

Figure 12-8 Parental Control : Bypass List

Table 12-6 Parental Control : Bypass List

LABEL	DESCRIPTION
-------	-------------



**Table 12-6 Parental Control : Bypass List**

LABEL	DESCRIPTION
Name	Type a name to identify a device on your LAN.
MAC Address	Type the MAC address (with colons) of a device on your LAN.
Apply	Click <b>Apply</b> to save your changes back to the HomeSafe.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# Chapter 13

## Firewall

*This chapter gives some background information on firewalls and explains how to get started with the HomeSafe firewall.*

### 13.1 Introduction

#### What is a Firewall?

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

#### Stateful Inspection Firewall.

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

#### About the HomeSafe Firewall

The HomeSafe firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click **FIREWALL** and then click the **Enable Firewall** check box). The HomeSafe's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The HomeSafe can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The HomeSafe is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The HomeSafe has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.

The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

#### 13.1.1 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.

4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

## 13.2 Firewall Settings Screen

From the **MAIN MENU**, click **FIREWALL** to open the **Settings** screen.

**FIREWALL**

**Settings** **Services**

☒ **Enable Firewall**

☒ **Bypass Triangle Route**

Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

1. LAN to WAN  
All traffic originating from the LAN is forwarded unless you block certain services in the Services screen. All blocked LAN-to-WAN packets are considered alerts. Packets to Log

2. WAN to LAN  
All traffic originating from the WAN is blocked unless you configure port forwarding rules, One-to-One mapping rules, Many-One-to-One mapping rules and/or allow remote management. Forwarded WAN-to-LAN packets are not considered alerts. Packets to Log

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

**Trusted Computer IP Address:**

**Figure 13-1 Firewall: Settings**

The following table describes the labels in this screen.

**Table 13-1 Firewall: Settings**

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The HomeSafe performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the HomeSafe firewall ignore the use of triangle route topology on the network. See the appendix for more on triangle route topology.
LAN to WAN	To log packets related to firewall rules, make sure that <b>Access Control</b> under <b>Log</b> is selected in the <b>Logs, Log Settings</b> screen.

Table 13-1 Firewall: Settings

LABEL	DESCRIPTION
Packets to Log	Choose what <b>LAN to WAN</b> packets to log. Choose from: <ul style="list-style-type: none"> <li>➤ <b>No Log</b></li> <li>➤ <b>Log Blocked</b> (blocked LAN to WAN services appear in the <b>Blocked Services</b> textbox in the <b>Services</b> screen (with <b>Enable Services Blocking</b> selected))</li> <li>➤ <b>Log All</b> (log all <b>LAN to WAN</b> packets)</li> </ul>
WAN to LAN	To log packets related to firewall rules, make sure that <b>Access Control</b> under <b>Log</b> is selected in the <b>Logs, Log Settings</b> screen.
Packets to Log	Choose what <b>WAN to LAN</b> and WAN to WAN/HomeSafe packets to log. Choose from: <ul style="list-style-type: none"> <li>➤ <b>No Log</b></li> <li>➤ <b>Log Forwarded</b> (see how to forward WAN to LAN traffic in the next section)</li> <li>➤ <b>Log All</b> (log all <b>WAN to LAN</b> packets).</li> </ul>
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
Apply	Click <b>Apply</b> to save the settings.
Reset	Click <b>Reset</b> to start configuring this screen again.

### 13.3 The Firewall, NAT and Remote Management

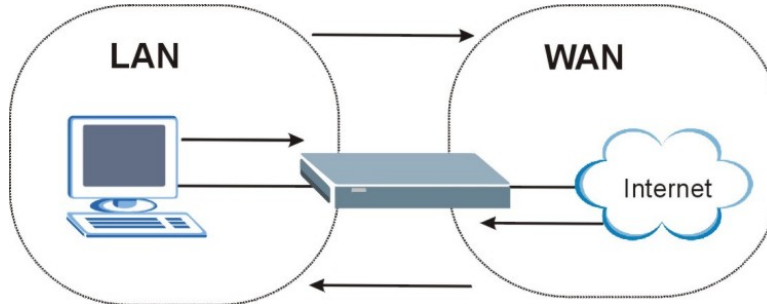


Figure 13-2 Firewall Rule Directions

#### 13.3.1 LAN-to-WAN rules

**LAN-to-WAN** rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

How can you block certain LAN to WAN traffic?

You may choose to block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets are considered alerts. Alerts are “higher priority logs” that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/HomeSafe means the LAN to the HomeSafe LAN interface. This is always allowed, as this is how you manage the HomeSafe from your local computer.

### 13.3.2 WAN-to-LAN rules

**WAN-to-LAN** rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.

Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.

Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/HomeSafe firewall rules. WAN-to-WAN/HomeSafe firewall rules are Internet to the HomeSafe WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/HomeSafe packets to log.

Allow NetBIOS traffic from the WAN to the LAN using the **WAN IP** web screen or SMT menu 24.8 commands. Forwarded **WAN-to-LAN** packets are not considered alerts.

## 13.4 Services

Click on the **Service** tab. The screen appears as shown next. Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Figure 13-3 Firewall: Service

The following table describes the labels in this screen.

Table 13-2 Firewall: Service

LABEL	DESCRIPTION
Enable Services Blocking	Select this check box to enable this feature.
Available Service	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click <b>Add</b> to add the port to the <b>Blocked Service</b> field.
Blocked Service	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized port from the drop down list box.
Custom Port	A custom port is a service that is not available in the pre-defined <b>Available Services</b> list and you must define using the next two fields.
Type	Services are either <b>TCP</b> and/or <b>UDP</b> . Select from either <b>TCP</b> or <b>UDP</b> .
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the <b>Available Services</b> drop-down list and then click <b>Add</b> to add a service to the Blocked Service.
Delete	Select a service from the <b>Blocked Services List</b> and then click <b>Delete</b> to remove this service from the list.

**Table 13-2 Firewall: Service**

<b>LABEL</b>	<b>DESCRIPTION</b>
Clear All	Click <b>Clear All</b> to empty the <b>Blocked Service</b> .
Day to Block:	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the <b>All Day</b> check box. You can also configure specific times that by entering the start time in the <b>Start (hr)</b> and <b>Start (min)</b> fields and the end time in the <b>End (hr)</b> and <b>End (min)</b> fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click <b>Apply</b> to save the settings.
Reset	Click <b>Reset</b> to start configuring this screen again.



---

# Part V:

---

## Remote Management

---

This part provides information and configuration instructions for configuration of remote management.



# Chapter 14

## Remote Management Screens

*This chapter provides information on the Remote Management screens.*

### 14.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which HomeSafe interface (if any) from which computers.



**When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.**

---

You may manage your HomeSafe from a remote location via:

- |                       |                      |
|-----------------------|----------------------|
| ➤ Internet (WAN only) | ➤ ALL (LAN and WAN)  |
| ➤ LAN only,           | ➤ Neither (Disable). |
- 



**When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.**

---

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The HomeSafe automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. Telnet
3. HTTP

#### 14.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in one of the remote management screens.

3. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the HomeSafe will disconnect the session immediately.
4. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
5. There is a firewall rule that blocks it.

### 14.1.2 Remote Management and NAT

When NAT is enabled:

- Use the HomeSafe's WAN IP address when configuring from the WAN.
- Use the HomeSafe's LAN IP address when configuring from the LAN.

### 14.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The HomeSafe automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

You can change the timeout period in the **System** screen

## 14.2 Configuring WWW

To change your HomeSafe's World Wide Web settings, click **REMOTE MGMT** to display the **WWW** screen.

The screenshot shows the 'REMOTE MANAGEMENT' window with the 'WWW' tab selected. The 'WWW' section contains the following fields and controls:

- Server Port:** A text input field containing '80'.
- Server Access:** A dropdown menu currently set to 'LAN'.
- Secured Client IP Address:** A section with two radio buttons, 'All' (selected) and 'Selected'.
- Selected:** A text input field containing '0.0.0.0'.
- Buttons:** 'Apply' and 'Reset' buttons at the bottom.

**Figure 14-1 Remote Management : WWW**

The following table describes the labels in this screen.

**Table 14-1 Remote Management : WWW**

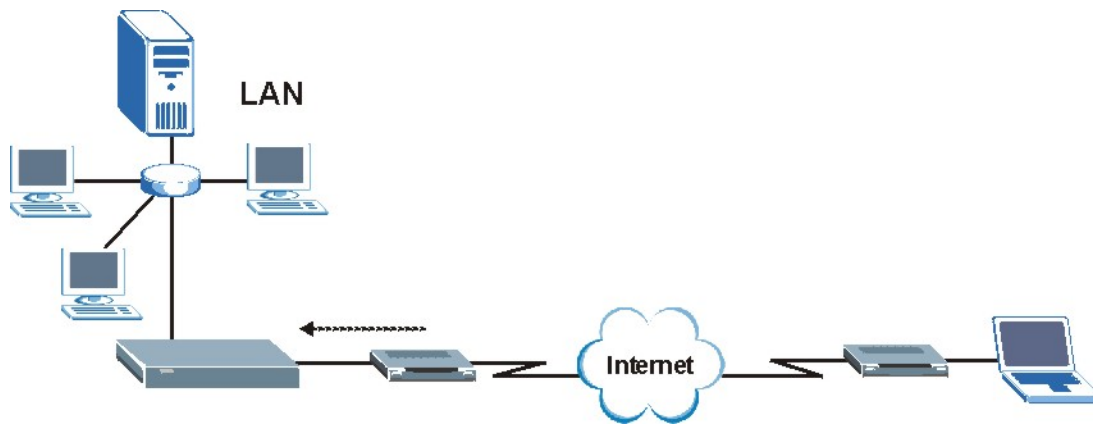
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

**Table 14-1 Remote Management : WWW**

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the HomeSafe using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the HomeSafe using this service. Select <b>All</b> to allow any computer to access the HomeSafe using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the HomeSafe using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 14.3 Configuring Telnet

You can configure your HomeSafe for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the HomeSafe.

**Figure 14-2 Telnet Configuration on a TCP/IP Network**

### 14.4 Configuring TELNET

Click **REMOTE MGMT** and the **TELNET** tab to display the screen as shown.

Figure 14-3 Remote Management : Telnet

The following table describes the labels in this screen.

Table 14-2 Remote Management : Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the HomeSafe using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the HomeSafe using this service. Select <b>All</b> to allow any computer to access the HomeSafe using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the HomeSafe using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.5 Configuring FTP

You can upload and download the HomeSafe’s firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your HomeSafe’s FTP settings, click **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

Figure 14-4 Remote Management : FTP

The following table describes the labels in this screen.

Table 14-3 Remote Management : FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the HomeSafe using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the HomeSafe using this service. Select <b>All</b> to allow any computer to access the HomeSafe using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the HomeSafe using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.6 SNMP

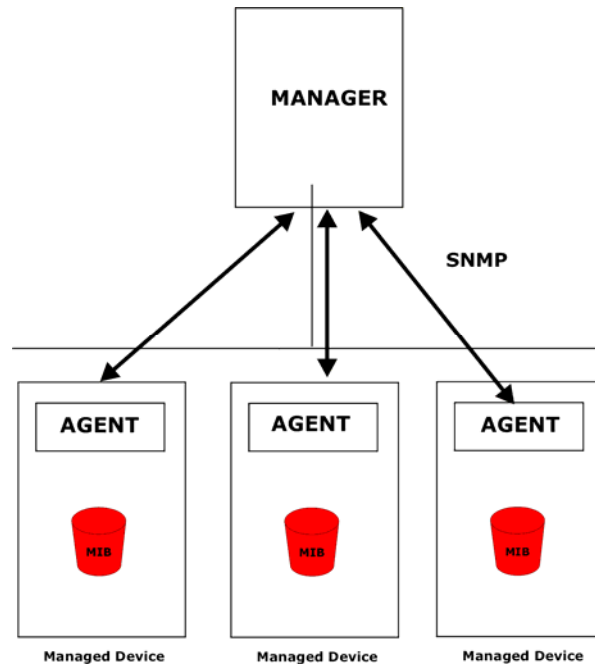
Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your HomeSafe supports SNMP agent functionality, which allows a manager station to manage and monitor the HomeSafe through the network. The HomeSafe supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.



---

**SNMP is only available if TCP/IP is configured.**

---



**Figure 14-5 SNMP Management Model**

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the HomeSafe). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.



### 14.6.1 Supported MIBs

The HomeSafe supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### 14.6.2 SNMP Traps

The HomeSafe will send traps to the SNMP manager when any one of the following events occurs:

**Table 14-4 SNMP Traps**

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

### 14.6.3 Configuring SNMP

To change your HomeSafe's SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

**REMOTE MANAGEMENT**

TELNET FTP WWW **SNMP** DNS Security

**SNMP Configuration**

Get Community public

Set Community public

Trusted Host 0.0.0.0

Trap Community public

Destination 0.0.0.0

**SNMP**

Service Port 161

Service Access LAN

Secured Client IP Address ☒ All ☐

Selected 0.0.0.0

Apply Reset

Figure 14-6 Remote Management : SNMP

The following table describes the labels in this screen.

Table 14-5 Remote Management : SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trusted Host	If you enter a trusted host, your HomeSafe will only respond to SNMP messages from this address. A blank (default) field means your HomeSafe will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

**Table 14-5 Remote Management : SNMP**

LABEL	DESCRIPTION
Service Access	Select the interface(s) through which a computer may access the HomeSafe using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the HomeSafe using this service. Select <b>All</b> to allow any computer to access the HomeSafe using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the HomeSafe using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

To change your HomeSafe's DNS settings, click **REMOTE MGMT**, then the **DNS** tab. The screen appears as shown.

The screenshot shows the 'REMOTE MANAGEMENT' window with the 'DNS' tab selected. The 'Service Port' is set to 53. The 'Service Access' is set to 'LAN'. The 'Secured Client IP Address' section has 'All' selected and the IP address '0.0.0.0' entered. 'Apply' and 'Reset' buttons are at the bottom.

**Figure 14-7 Remote Management : DNS**

The following table describes the labels in this screen.

**Table 14-6 Remote Management : DNS**

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the HomeSafe.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to send DNS queries to the HomeSafe. Select <b>All</b> to allow any computer to send DNS queries to the HomeSafe. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send DNS queries to the HomeSafe.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.8 Configuring Security

To change your HomeSafe's security settings, click **REMOTE MGMT**, then the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your HomeSafe, an ICMP response packet is automatically returned. This allows the outside user to know the HomeSafe exists. Your HomeSafe supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your HomeSafe when unsupported ports are probed.

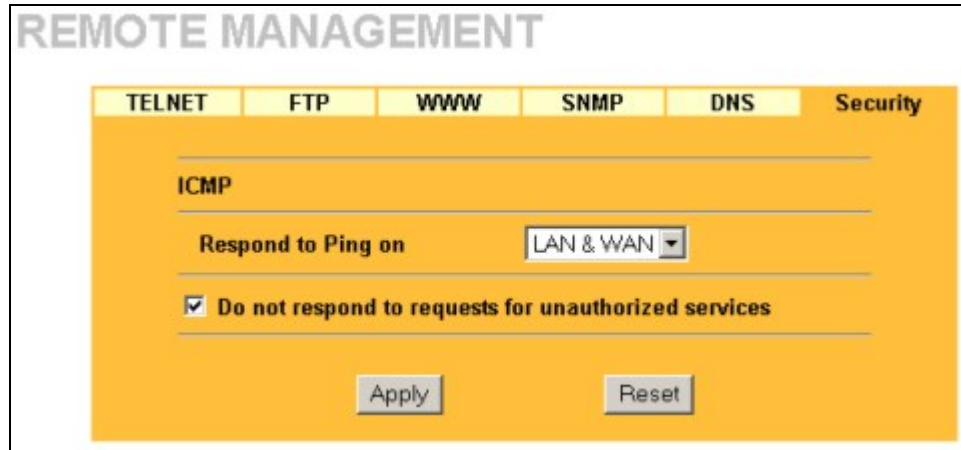


Figure 14-8 Remote Management : Security

The following table describes the labels in this screen.

Table 14-7 Remote Management : Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The HomeSafe will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the HomeSafe by probing for unused ports. If you select this option, the HomeSafe will not respond to port request(s) for unused ports, thus leaving the unused ports and the HomeSafe unseen. By default this option is not selected and the HomeSafe will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.  Note that the probing packets must first traverse the HomeSafe's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the HomeSafe reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.

**Table 14-7 Remote Management : Security**

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.





---

## Part VI:

---

### Logs and Maintenance

---

This part covers the centralized logs and maintenance screens.



# Chapter 15

## Centralized Logs

*This chapter contains information about configuring general log settings and viewing the HomeSafe's logs. Refer to the appendices for example log message explanations.*

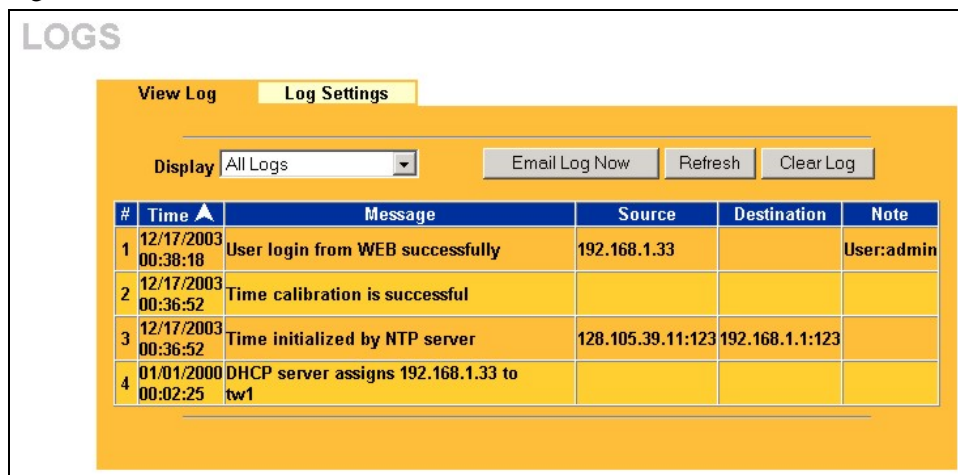
### 15.1 View Log

The web configurator allows you to look at all of the HomeSafe's logs in one location.

Click the **LOGS** in the navigation panel to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 15.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.



**Figure 15-1 View Logs**

The following table describes the labels in this screen.

**Table 15-1 View Logs**

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> page (see <i>section 15.2</i> ) display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the HomeSafe's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.

**Table 15-1 View Logs**

LABEL	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>Address Info</b> fields in <b>Log Settings</b> , see <i>section 15.2</i> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.

## 15.2 Log Settings

You can configure the HomeSafe's general log settings in one location.

Click the **LOGS** in the navigation panel and then the **Log Settings** tab to open the **Log Settings** screen.

Use the **Log Settings** screen to configure to where the HomeSafe is to send logs; the schedule for when the HomeSafe is to send the logs and which logs and/or immediate alerts the HomeSafe to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent

Log Settings

View Log

Log Settings

Address Info:

Mail Server:

(Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send log to:

(E-Mail Address)

Send alerts to:

(E-Mail Address)

Syslog Logging:

☐ Active

Syslog IP Address:

0.0.0.0

(Server NAME or IP Address)

Log Facility:

Local 1

Send Log:

Log Schedule:

None

Day for Sending Log:

Sunday

Time for Sending Log:

0 (hour) 0 (minute)

☐ Clear log after sending mail

Log

☒ System Maintenance

☒ System Errors

☐ Access Control

☐ TCP Reset

☐ Packet Filter

☐ ICMP

☐ Remote Management

☒ CDR

☒ PPP

☐ UPnP

☐ Forward Web Sites

☐ Blocked Web Sites

☐ Blocked Java etc.

☐ Attacks

☐ 802.1x

☐ Wireless

☐ Any IP

☐ Parental Control

Send immediate alert

☐ System Errors

☐ Access Control

☐ Blocked Web Sites

☐ Blocked Java etc.

☐ Attacks

Apply

Reset

Figure 15-2 Log Settings

The following table describes the labels in this screen.

Table 15-2 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.

**Table 15-2 Log Settings**

LABEL	DESCRIPTION
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the HomeSafe sends. Not all HomeSafe models have this field.
Send Log To	The HomeSafe sends logs to the e-mail address specified in this field. If this field is left blank, the HomeSafe does not send logs via e-mail.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the e-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	The HomeSafe sends a log to an external syslog server.
Active	Click <b>Active</b> to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Send Log	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"><li>• <b>Daily</b></li><li>• <b>Weekly</b></li><li>• <b>Hourly</b></li><li>• <b>When Log is Full</b></li><li>• <b>None.</b></li></ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the E-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b>, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to remove any logs that are recorded in the view logs page after they are sent by E-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the HomeSafe to send e-mail alerts immediately.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Chapter 16

## Maintenance

*This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.*

### 16.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your HomeSafe.

### 16.2 Status Screen

Click **MAINTENANCE** to open the **Status** screen, which you can use to monitor your HomeSafe. Note that these fields are READ-ONLY and only for diagnostic purposes.

**SYSTEM STATUS**

[Status](#)
[DHCP Table](#)
[Any IP](#)
[Association List](#)
[F/W Upload](#)
[Configuration](#)
[Restart](#)

System Name : HS-100W

Model Name : HS-100/HS-100W  
 ZyNOS Firmware Version: V3.60(JM.0)b1 | 05/17/2004  
 Routing Protocols :IP

WAN Port :

IP Address : 172.21.3.125      DHCP : Client  
 IP Subnet Mask : 255.255.0.0

LAN Port :

IP Address : 192.168.1.1      DHCP : Server  
 IP Subnet Mask : 255.255.255.0

Show Statistics

**Figure 16-1 Maintenance : Status**

The following table describes the labels in this screen.

**Table 16-1 Maintenance : Status**

LABEL	DESCRIPTION
System Name	This is the <b>System Name</b> you chose in the first Internet Access Wizard screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name should also be on a sticker on your HomeSafe. If you are uploading firmware, be sure to upload firmware for this exact model name. This field is not available on all models.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol - <b>IP</b> for which the HomeSafe is configured. This field is not configurable in all HomeSafe router models.
WAN Port	
IP Address	This is the WAN port IP address.

**Table 16-1 Maintenance : Status**

LABEL	DESCRIPTION
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - <b>Client</b> or <b>None</b> .
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - <b>Server</b> , <b>Relay</b> or <b>None</b> .
Show Statistics	Click <b>Show Statistics</b> to display the real-time system statistics. Refer to <i>Section 16.2.1</i> for more information.

### 16.2.1 System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	3494	3404	0	0	0	2:16:35
WLAN	216	824	0	0	0	0	2:16:35

System Up Time : 2:16:40

Poll Interval :  sec

**Figure 16-2 Maintenance : System Statistics**

The following table describes the labels in this screen.

**Table 16-2 Maintenance : System Statistics**

LABEL	DESCRIPTION
Port	This is the WAN, LAN or WLAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the HomeSafe has been on.

**Table 16-2 Maintenance : System Statistics**

LABEL	DESCRIPTION
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics, click <b>Stop</b> .

### 16.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the HomeSafe as a DHCP server or disable it. When configured as a server, the HomeSafe provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	tw11477-02	00:50:8d:48:59:1f	<input checked="" type="checkbox"/>

**Figure 16-3 Maintenance : DHCP Table**

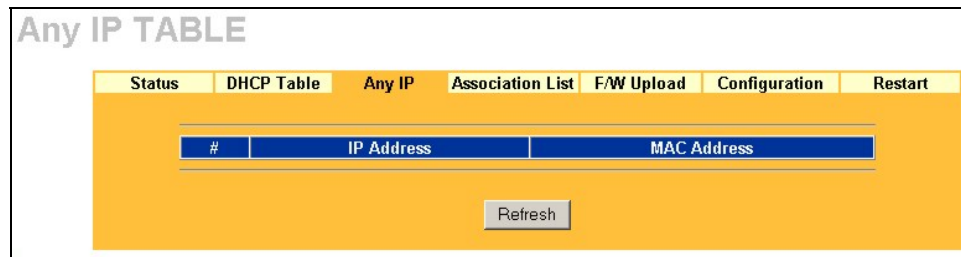
The following table describes the labels in this screen.

**Table 16-3 Maintenance : DHCP Table**

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this check box to have the HomeSafe always assign this IP address to this MAC address (and host name).
Apply	Click <b>Apply</b> to have the MAC address and IP address also display in the <b>LAN Static DHCP</b> screen (where you can edit them).
Refresh	Click <b>Refresh</b> to renew the screen.

## 16.4 Any IP Table

Click **MAINTENANCE**, **Any IP Table**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the HomeSafe.



**Figure 16-4 Maintenance : Any IP**

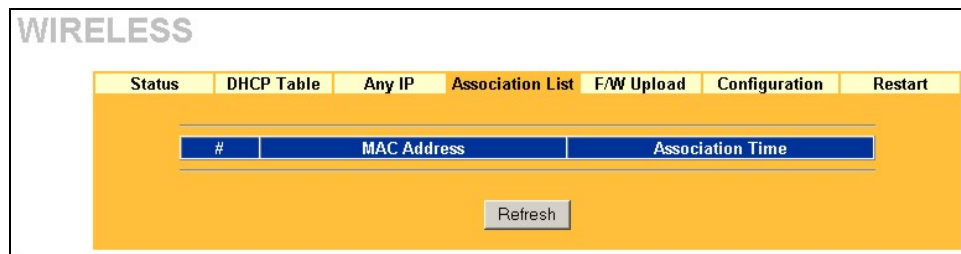
The following table describes the labels in this screen.

**Table 16-4 Maintenance : Any IP**

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click <b>Refresh</b> to update this screen.

## 16.5 Association List

View the wireless stations that are currently associated to the HomeSafe in the **Association List** screen.



**Figure 16-5 Maintenance : Association List**

The following table describes the labels in this screen.

**Table 16-5 Maintenance : Association List**

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.



Table 16-5 Maintenance : Association List

LABEL	DESCRIPTION
Association Time	This field displays the time a wireless station first associated with the HomeSafe.
Refresh	Click <b>Refresh</b> to redisplay the current screen.

## 16.6 F/W Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a "\*.bin" extension, e.g., "HomeSafe.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the *Firmware and Configuration File Maintenance* chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **F/W Upload** tab. Follow the instructions in this screen to upload firmware to your HomeSafe.

Figure 16-6 Maintenance : Firmware Upload

The following table describes the labels in this screen.

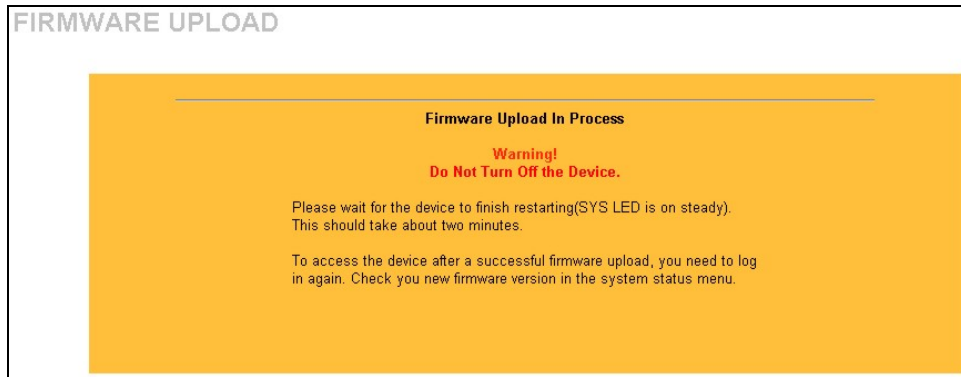
Table 16-6 Maintenance : Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.



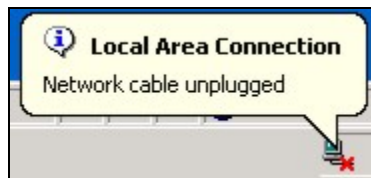
**Do not turn off the HomeSafe while firmware upload is in progress!**

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the HomeSafe again.



**Figure 16-7 Upload Warning**

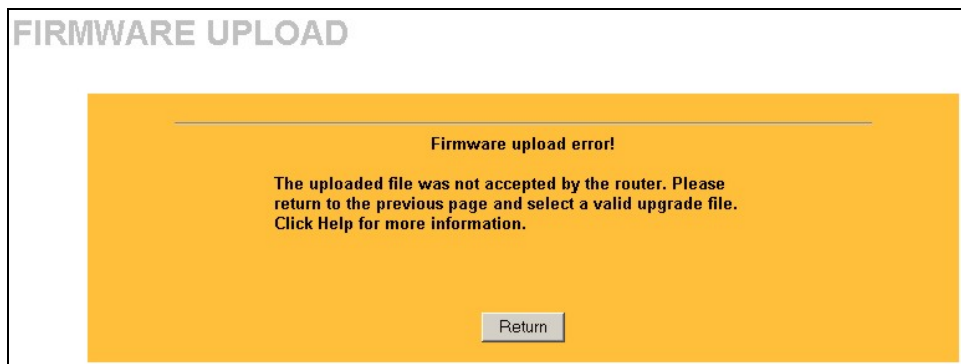
The HomeSafe automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



**Figure 16-8 Network Temporarily Disconnected**

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.



**Figure 16-9 Upload Error Message**

## 16.7 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**MAINTENANCE**

Status DHCP Table Any IP Association List F/W Upload **Configuration** Restart

**Backup Configuration**

Click Backup to save the current configuration of your system to your computer.

Backup

**Restore Configuration**

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:  Browse...

Upload

**Back to Factory Defaults**

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Reset

Figure 16-10 Maintenance : Configuration

### 16.7.1 Backup Configuration

Backup configuration allows you to back up (save) the HomeSafe's current configuration to a file on your computer. Once your HomeSafe is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the HomeSafe's current configuration to your computer

### 16.7.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your HomeSafe.

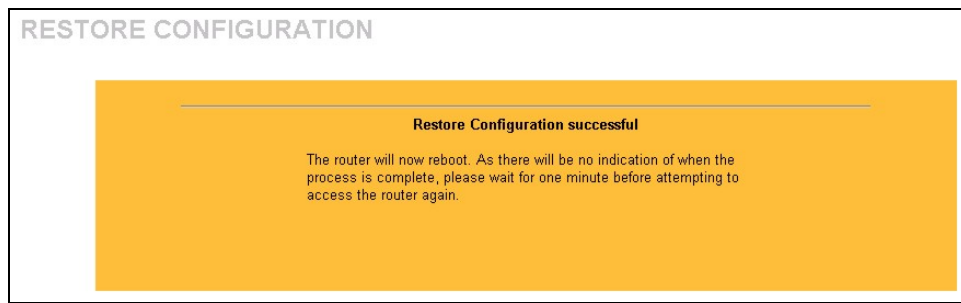
Table 16-7 Maintenance : Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.



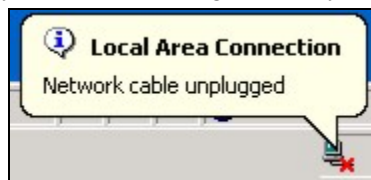
**Do not turn off the HomeSafe while configuration file upload is in progress.**

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the HomeSafe again.



**Figure 16-11 Configuration : Restore Successful**

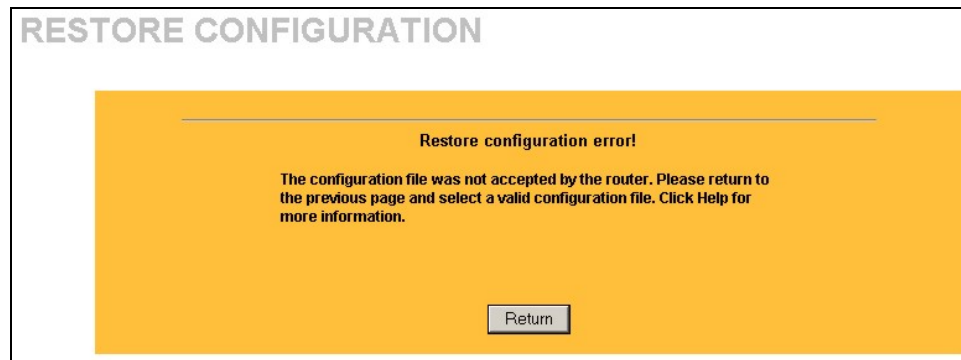
The HomeSafe automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



**Figure 16-12 Temporarily Disconnected**

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default HomeSafe IP address (192.168.1.1). See your *Quick Start Guide* for details on how to set up your computer's IP address.

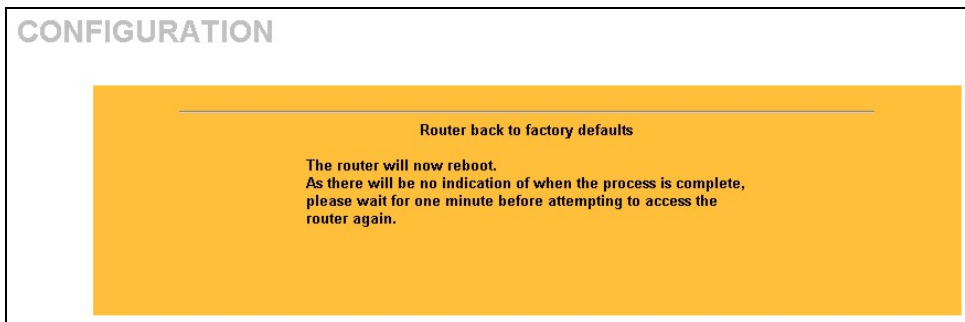
If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.



**Figure 16-13 Configuration Restore Error**

### 16.7.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the HomeSafe to its factory defaults as shown on the screen. The following warning screen will appear.



**Figure 16-14 Factory Defaults**

You can also press the **RESET** button on the rear panel to reset the factory defaults of your HomeSafe. Refer to the *Hardware Installation* chapter for more information on the **RESET** button.

## 16.8 Restart Screen

System restart allows you to reboot the HomeSafe without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the HomeSafe reboot. This does not affect the HomeSafe's configuration.



**Figure 16-15 Maintenance : System Restart**

---

---

# Part VII:

---

## SMT General Configuration

---

This part covers System Management Terminal configuration for general setup, WAN setup, LAN setup, WLAN setup, Internet access, remote node, static route, NAT and enabling the firewall.



**See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.**

---



# Chapter 17

## Introducing the SMT

*This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.*

### 17.1 SMT Introduction

The HomeSafe's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

#### 17.1.1 Procedure for SMT Configuration via Console Port

Follow the steps below to access your HomeSafe via the console port.

Configure a terminal emulation communications program as follows: VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, data flow set to none, 9600 bps port speed.

Press [ENTER] to display the SMT password screen. The default password is "1234".

#### 17.1.2 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your HomeSafe.

**Step 1.** In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.

**Step 2.** Enter "1234" in the **Password** field.

**Step 3.** After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your HomeSafe will automatically log you out. You will then have to telnet into the HomeSafe again.

#### 17.1.3 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "\*" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your HomeSafe will automatically log you out.



**Figure 17-1 Login Screen**

#### 17.1.4 HomeSafe SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your HomeSafe.



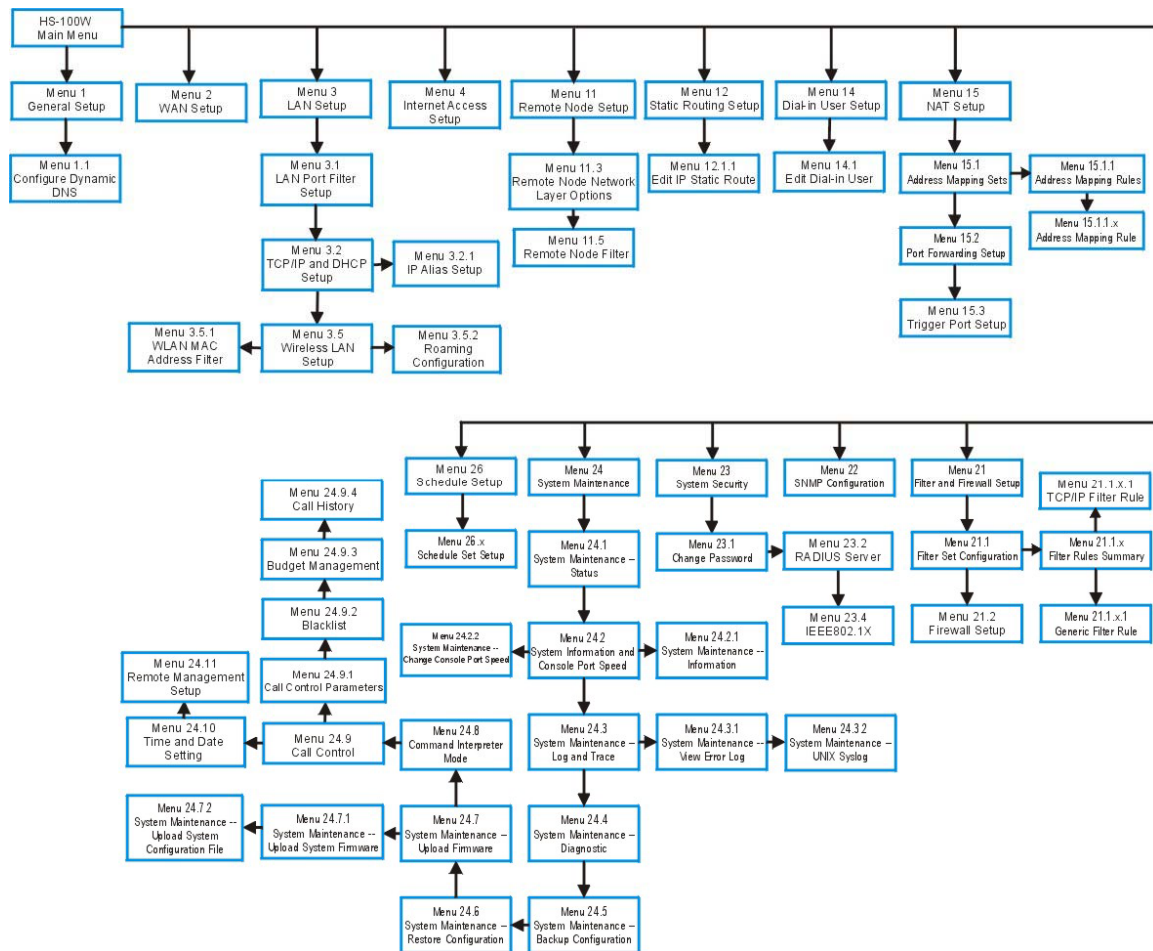


Figure 17-2 SMT Menu Overview

## 17.2 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your HomeSafe.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 17-1 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change <b>No</b> to <b>Yes</b> then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of <b>No</b> . Press [SPACE BAR] once to change <b>No</b> to <b>Yes</b> , and then press [ENTER] to go to the “hidden” menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.

**Table 17-1 Main Menu Commands**

Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? > or <b>ChangeMe</b>	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with <b>ChangeMe</b> must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.	
HS-100/HS-100W Main Menu	
Getting Started	Advanced Management
1. General Setup	21. Filter and Firewall Setup
2. WAN Setup	22. SNMP Configuration
3. LAN Setup	23. System Security
4. Internet Access Setup	24. System Maintenance
	26. Schedule Setup
Advanced Applications	
11. Remote Node Setup	
12. Static Routing Setup	
14. Dial-in User Setup	
15. NAT Setup	
	99. Exit
Enter Menu Selection Number:	

**Figure 17-3 SMT Main Menu**

## 17.2.1 System Management Terminal Interface Summary

**Table 17-2 Main Menu Summary**

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Use this menu to set up static routes.

**Table 17-2 Main Menu Summary**

#	MENU TITLE	DESCRIPTION
14	Dial-in User Setup	Use this menu to set up local user profiles on the HomeSafe.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

### 17.3 Changing the System Password

Change the HomeSafe default password by following the steps shown next.

**Step 1.** Enter 23 in the main menu to display **Menu 23 - System Security** as shown next.

```

Menu 23 - System Security

1. Change Password
2. RADIUS Server

4. IEEE802.1x

```

**Step 1.** Enter 23.1 in the main menu to display **Menu 23.1 - System Security - Change Password**.

**Step 3.** Type your existing system password in the **Old Password** field, for example “1234”, and press [ENTER].

```

Menu 23.1 - System Security - Change Password

Old Password= ?
New Password= ?
Retype to confirm= ?

```

**Figure 17-4 Menu 23 System Password**

**Step 4.** Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

**Step 5.** Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “\*” for each character you type.

# Chapter 18

## Menu 1 General Setup

*Menu 1 - General Setup contains administrative and system-related information.*

### 18.1 General Setup

**Menu 1 — General Setup** contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the HomeSafe **System Name**.
- In Windows 2000 click **Start, Settings, Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the HomeSafe **System Name**.
- In Windows XP, click **start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the HomeSafe **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the HomeSafe via DHCP.

### 18.2 Procedure To Configure Menu 1

**Step 1.** Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next).

Menu 1 - General Setup

System Name= HS-100W  
Domain Name= zyxel.com.tw

First System DNS Server= From ISP  
IP Address= N/A  
Second System DNS Server= From ISP  
IP Address= N/A  
Third System DNS Server= From ISP  
IP Address= N/A  
Edit Dynamic DNS= No

**Figure 18-1 Menu 1 General Setup**

**Step 2.** Fill in the required fields. Refer to the table shown next for more information about these fields.

**Table 18-1 Menu 1 General Setup**

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	

**Table 18-1 Menu 1 General Setup**

<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router.  The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].	zyxel.com.tw
First System DNS Server Second System DNS Server Third System DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The HomeSafe uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.  Press [SPACE BAR] and then [ENTER] to select an option. Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the HomeSafe's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns. Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the <b>IP Address</b> field. If you select <b>User-Defined</b> , but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you save your changes. If you set a second choice to <b>User-Defined</b> , and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you save your changes. Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.	<b>From ISP</b>
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> (default). Select <b>Yes</b> to configure <b>Menu 1.1: Configure Dynamic DNS</b> discussed next.	<b>No</b> (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

## 18.2.1 Procedure to Configure Dynamic DNS



**If you have a private WAN IP address, then you cannot use Dynamic DNS.**

- Step 1.** To configure Dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
DDNS Type= DynamicDNS
Host Name 1=
Host Name 2=
Host Name 3=
Username=
Password= *****
Enable Wildcard Option= No
Enable Off Line Option= N/A
IP Address Update Policy:
  DDNS Server Auto Detect IP Address= No
  Use Specified IP Address= No
  Use IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

**Figure 18-2 Menu 1.1 Configure Dynamic DNS**

Follow the instructions in the next table to configure Dynamic DNS parameters.

**Table 18-2 Menu 1.1 Configure Dynamic DNS**

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to make dynamic DNS active.	<b>Yes</b>
DDNS Type	Press [SPACE BAR] and then [ENTER] to select <b>DynamicDNS</b> if you have a dynamic IP address(es). Select <b>StaticDNS</b> if you have a static IP address(s). Select <b>CustomDNS</b> to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	<b>DynamicDNS</b> (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard Option	Your HomeSafe supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> This field is <b>N/A</b> when you choose DDNS client as your service provider.	<b>No</b>
Enable Off Line Option	This field is only available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> . When <b>Yes</b> is selected, <a href="http://www.dyndns.org/">http://www.dyndns.org/</a> traffic is redirected to a URL that you have previously specified (see <a href="http://www.dyndns.org/">www.dyndns.org</a> for details).	<b>Yes</b>

**Table 18-2 Menu 1.1 Configure Dynamic DNS**

FIELD	DESCRIPTION	EXAMPLE
<p>IP Address Update Policy:</p> <p>You can select <b>Yes</b> in either the <b>Use Server Detected IP</b> field (recommended) or the <b>User Specified IP Addr</b> field, but not both.</p> <p>With the <b>Use Server Detected IP</b> and <b>User Specified IP Addr</b> fields both set to <b>No</b>, the DDNS server automatically updates the IP address of the host name(s) with the HomeSafe's WAN IP address.</p> <p>DDNS does not work with a private IP address. When both fields are set to <b>No</b>, the HomeSafe must have a public WAN IP address in order for DDNS to work.</p>		
DDNS Server Auto Detect IP Address	<p>Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the HomeSafe uses or is behind.</p> <p>You can set this field to <b>Yes</b> whether the IP address is public or private, static or dynamic.</p>	<b>Yes</b>
Use Specified IP Address	<p>Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.</p> <p>Only select <b>Yes</b> if the HomeSafe uses or is behind a static public IP address.</p>	<b>No</b>
Use IP Address	Enter the static public IP address if you select <b>Yes</b> in the <b>Use Specified IP Address</b> field.	<b>N/A</b>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.</p>		

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

# Chapter 19

## Menu 2 WAN Setup

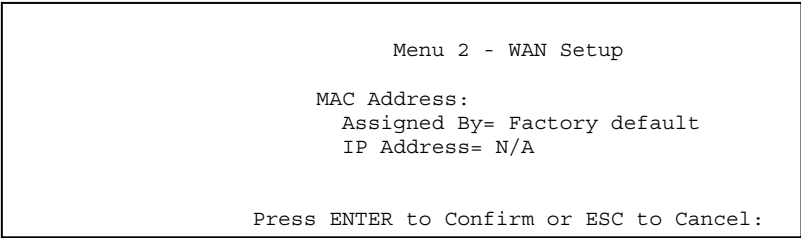
*This chapter describes how to configure the WAN using menu 2.*

### 19.1 Introduction to WAN

This chapter explains how to configure settings for your WAN port.

### 19.2 WAN Setup

From the main menu, enter 2 to open menu 2.



**Figure 19-1 Menu 2 WAN Setup**

The following table describes the fields in this menu.

**Table 19-1 Menu 2 WAN Setup**

FIELD	DESCRIPTION
MAC Address	
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose <b>Factory Default</b> to select the factory assigned default MAC Address. Choose <b>IP address attached on LAN</b> to use the MAC Address of that computer whose IP you give in the following field.
IP Address	This field is applicable only if you choose the <b>IP address attached on LAN</b> method in the <b>Assigned By</b> field. Enter the IP address of the computer on the LAN whose MAC you are cloning.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	





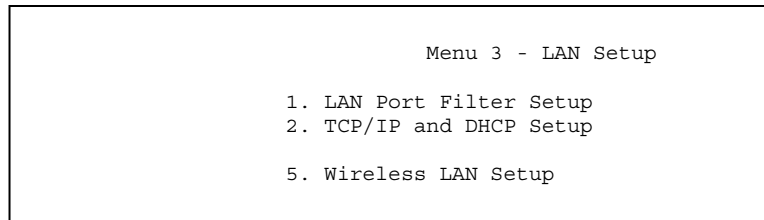
# Chapter 20

## Menu 3 LAN Setup

*This chapter covers how to configure your wired Local Area Network (LAN) settings.*

### 20.1 LAN Setup

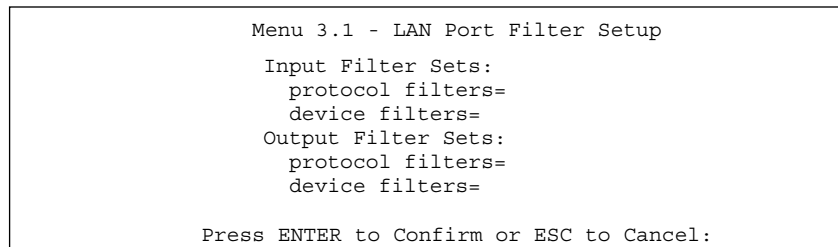
This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.



**Figure 20-1 Menu 3 LAN Setup**

#### 20.1.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.



**Figure 20-2 Menu 3.1 LAN Port Filter Setup**

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

### 20.2 Protocol Dependent Ethernet Setup

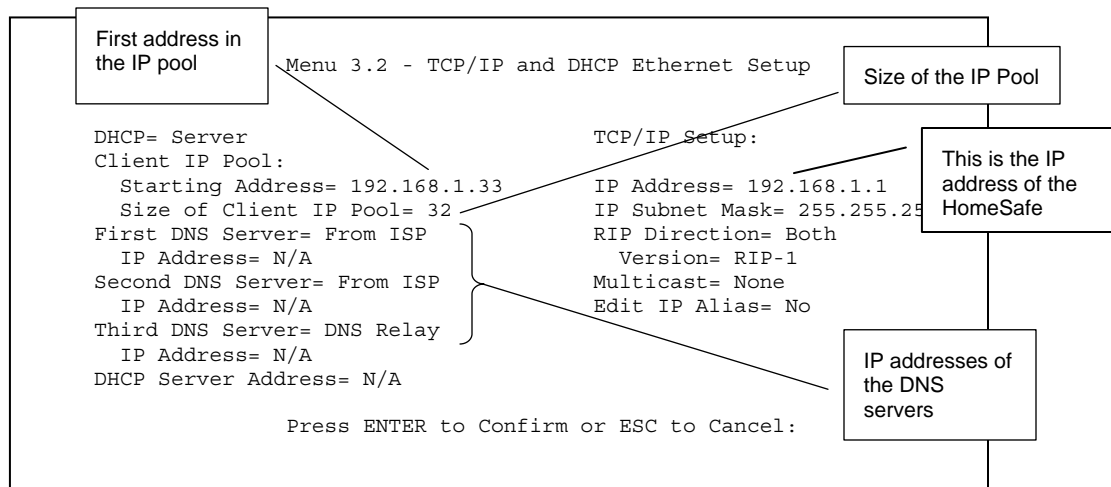
Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to the *Internet Access Application* chapter.
- For bridging Ethernet setup refer to the *Bridging Setup* chapter.

### 20.3 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your HomeSafe for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

**Figure 20-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup**

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 20-1 Menu 3.2: DHCP Ethernet Setup Fields**

FIELD	DESCRIPTION	EXAMPLE
DHCP	This field enables/disables the DHCP server. If set to <b>Server</b> , your HomeSafe will act as a DHCP server. If set to <b>None</b> , the DHCP server will be disabled. If set to <b>Relay</b> , the HomeSafe acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to <b>Server</b> , the following items need to be set:	<b>Server</b>
Client IP Pool:		
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	128

**Table 20-1 Menu 3.2: DHCP Ethernet Setup Fields**

<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
First DNS Server Second DNS Server Third DNS Server	<p>The HomeSafe passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.</p> <p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the HomeSafe's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the <b>IP Address</b> field below. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you save your changes. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you save your changes.</p> <p>Select <b>DNS Relay</b> to have the HomeSafe act as a DNS proxy. The HomeSafe's LAN IP address displays in the <b>IP Address</b> field below (read-only). The HomeSafe tells the DHCP clients on the LAN that the HomeSafe itself is the DNS server. When a computer on the LAN sends a DNS query to the HomeSafe, the HomeSafe forwards the query to the HomeSafe's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to <b>None</b> after you save your changes.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>	<b>From ISP</b>
DHCP Server Address	If <b>Relay</b> is selected in the <b>DHCP</b> field above, then type the IP address of the actual, remote DHCP server here.	

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

**Table 20-2 Menu 3.2: LAN TCP/IP Setup Fields**

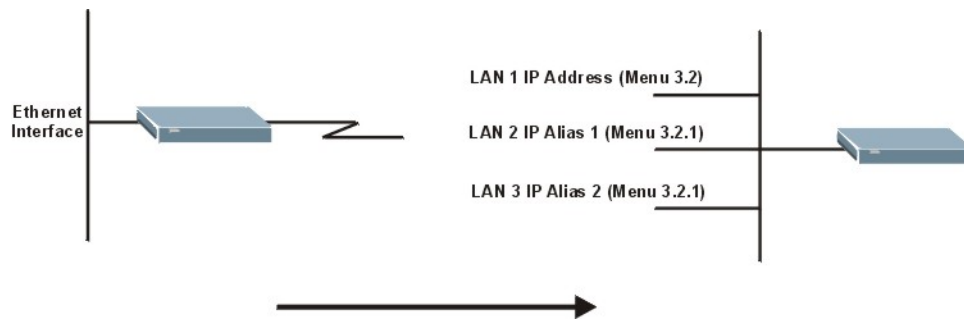
<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
TCP/IP Setup:		
IP Address	Enter the IP address of your HomeSafe in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your HomeSafe will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the HomeSafe.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: <b>Both</b> , <b>In Only</b> , <b>Out Only</b> or <b>None</b> .	<b>Both</b> (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: <b>RIP-1</b> , <b>RIP-2B</b> or <b>RIP-2M</b> .	<b>RIP-1</b> (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The HomeSafe supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select <b>None</b> (default) to disable it.	<b>None</b>

**Table 20-2 Menu 3.2: LAN TCP/IP Setup Fields**

FIELD	DESCRIPTION	EXAMPLE
Edit IP Alias	The HomeSafe supports three logical LAN interfaces via its single physical Ethernet interface with the HomeSafe itself as the gateway for each LAN network. Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to display menu 3.2.1	<b>No</b>
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.		

### 20.3.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The HomeSafe supports three logical LAN interfaces via its single physical Ethernet interface with the HomeSafe itself as the gateway for each LAN network.

**Figure 20-4 Physical Network & Partitioned Logical Networks**

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
  IP Address=
  IP Subnet Mask= 0.0.0.0
  RIP Direction= None
    Version= RIP-1
  Incoming protocol filters=
  Outgoing protocol filters=
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

**Figure 20-5 Menu 3.2.1: IP Alias Setup**

Use the instructions in the following table to configure IP alias parameters.

**Table 20-3 Menu 3.2.1: IP Alias Setup**

FIELD	DESCRIPTION	EXAMPLE
IP Alias 1, 2	Choose <b>Yes</b> to configure the LAN network for the HomeSafe.	<b>Yes</b>
IP Address	Enter the IP address of your HomeSafe in dotted decimal notation.	192.168.1.1
IP Subnet Mask	Your HomeSafe will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the HomeSafe.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are <b>Both, In Only, Out Only</b> or <b>None</b> .	<b>None</b>
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are <b>RIP-1, RIP-2B</b> or <b>RIP-2M</b> .	<b>RIP-1</b>
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the HomeSafe.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the HomeSafe.	2
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.		

## 20.4 Wireless LAN Setup

Use menu 3.5 to set up your HomeSafe as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

Menu 3.5 - Wireless LAN Setup

ESSID= ZyXEL

Hide ESSID= No

Channel ID= CH06 2437MHz

RTS Threshold= 2432

Frag. Threshold= 2432

WEP Encryption= Disable

Default Key= N/A

Key1= N/A

Key2= N/A

Key3= N/A

Key4= N/A

Authen. Method= N/A

Edit MAC Address Filter= No

Edit Roaming Configuration= No

Preamble= Long

802.11 Mode= Mixed

Press ENTER to Confirm or ESC to Cancel:


**Figure 20-6 Menu 3.5 Wireless LAN Setup**

The following table describes the fields in this menu.

**Table 20-4 Menu 3.5 Wireless LAN Setup**

FIELD	DESCRIPTION	EXAMPLE
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP to which the wireless stations associate. Wireless stations associating to the	<b>Wireless</b>

**Table 20-4 Menu 3.5 Wireless LAN Setup**

<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
	AP must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.	
Hide ESSID	Press [SPACE BAR] and select <b>Yes</b> to hide the ESSID in the outgoing data frame so an intruder cannot obtain the ESSID through passive scanning.	<b>No</b>
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.	<b>CH06 2437MHz</b>
RTS Threshold	Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	<b>2432</b>
Frag. Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	<b>2432</b>
WEP Encryption	Select <b>Disable</b> to allow wireless stations to communicate with the access points without any data encryption. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.	<b>Disable</b>
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the HomeSafe and the wireless stations to communicate.	<b>1</b>
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the HomeSafe and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <hr/> <p> <b>Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.</b></p> <hr/>	<b>0x12345abcde</b>
Authen. Method	Press [SPACE BAR] to select <b>Auto</b> , <b>Open System Only</b> or <b>Shared Key Only</b> and press [ENTER]. This field is <b>N/A</b> if WEP is not activated. If WEP encryption is activated, the default setting is <b>Auto</b> .	<b>Auto</b>
Edit MAC Address Filter	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to proceed to a MAC address filter configuration screen.	
Edit Roaming Configuration	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to proceed to a roaming configuration screen.	
Preamble	Select a preamble type from the drop-down list menu. Choices are <b>Long</b> , <b>Short</b> and <b>Dynamic</b> . The default setting is <b>Dynamic</b> . See the section on preamble for more information.	<b>Long</b>

**Table 20-4 Menu 3.5 Wireless LAN Setup**

FIELD	DESCRIPTION	EXAMPLE
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the HomeSafe.</p> <p>Select <b>Mixed</b> to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the HomeSafe. The transmission rate of your HomeSafe might be reduced.</p>	<b>Mixed</b>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

### 20.4.1 Configuring MAC Address Filter

Your HomeSafe checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your HomeSafe.

**Step 2.** From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

```

Menu 3.5 - Wireless LAN Setup

ESSID= ZyXEL
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= Disable
Default Key= N/A
Key1= N/A
Key2= N/A
Key3= N/A
Key4= N/A
Authen. Method= N/A

Edit MAC Address Filter= Yes
Edit Roaming Configuration= No
Preamble= Long
802.11 Mode= Mixed

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 20-7 Menu 3.5 Wireless LAN Setup**

In the **Edit MAC Address Filtering** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.



```
Menu 3.5.1 - WLAN MAC Address Filter

Active= No
Filter Action= Allowed Association
MAC Address Filter
Address 1= 00:00:00:00:00:00
Address 2= 00:00:00:00:00:00
Address 3= 00:00:00:00:00:00
Address 4= 00:00:00:00:00:00
Address 5= 00:00:00:00:00:00
Address 6= 00:00:00:00:00:00
Address 7= 00:00:00:00:00:00
Address 8= 00:00:00:00:00:00
Address 9= 00:00:00:00:00:00
Address 10= 00:00:00:00:00:00
Address 11= 00:00:00:00:00:00
Address 12= 00:00:00:00:00:00

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 20-8 Menu 3.5.1 WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 20-5 Menu 3.5.1 WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select <b>Yes</b> and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the HomeSafe, press [SPACE BAR] to select <b>Deny Association</b> and press [ENTER]. MAC addresses not listed will be allowed to access the router.  The default action, <b>Allowed Association</b> , permits association with the HomeSafe. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the HomeSafe in these address fields.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

20.4.2 Configuring Roaming on the HomeSafe

Enable the roaming feature if you have two or more HomeSafe's on the same subnet. Follow the steps below to allow roaming on your HomeSafe.

- Step 1.** From the main menu, enter 3 to display **Menu 3 – LAN Setup**.
- Step 2.** Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

```

Menu 3.5 - Wireless LAN Setup

ESSID= ZyXEL
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP Encryption= Disable
Default Key= N/A
Key1= N/A
Key2= N/A
Key3= N/A
Key4= N/A
Authen. Method= N/A

Edit MAC Address Filter= No
Edit Roaming Configuration= Yes

Preamble= Long
802.11 Mode= Mixed

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 20-9 Menu 3.5 Wireless LAN Setup**

**Step 3.** Move the cursor to the **Edit Roaming Configuration** field. Press [SPACE BAR] to select **Yes** and then press [ENTER]. **Menu 3.5.2 – Roaming Configuration** displays as shown next.

```

Menu 3.5.2 - Roaming Configuration

Active= Yes
Port #= 3517

```

**Figure 20-10 Menu 3.5.2 Roaming Configuration**

The following table describes the fields in this menu.

**Table 20-6 Menu 3.5.2 Roaming Configuration**

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to enable roaming on the HomeSafe if you have two or more HomeSafe's on the same subnet.
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is <b>3517</b> . Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	



# Chapter 21

## Internet Access

*This chapter shows you how to configure your HomeSafe for Internet access .*

### 21.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your HomeSafe to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

### 21.2 Ethernet Encapsulation

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**.

If you choose **Ethernet** in menu 4 you will see the next menu.

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only
  
```

**Figure 21-1 Menu 4 Internet Access Setup**

The following table describes the fields in this menu.

**Table 21-1 Menu 4: Internet Access Setup (Ethernet)**

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>Ethernet</b> . The encapsulation method influences your choices for the <b>IP Address</b> field.
Service Type	Press [SPACE BAR] and then [ENTER] to select <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method), <b>RR-Telstra</b> or <b>Telia Login</b> . Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
Note: DSL users must choose the <b>Standard</b> option only. The <b>My Login</b> , <b>My Password</b> and <b>Login Server</b> fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.

**Table 21-1 Menu 4: Internet Access Setup (Ethernet)**

FIELD	DESCRIPTION
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The HomeSafe will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Relogin Every (min)	This field is available when you select <b>Telia Login</b> in the <b>Service Type</b> field. The Telia server logs the HomeSafe out if the HomeSafe does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the HomeSafe to wait between logins.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> , otherwise select <b>Static</b> and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose <b>None</b> to disable NAT. Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b> . Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b> , <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b> , <b>Many- One-to-One</b> and <b>Server</b> . When you select <b>Full Feature</b> you must configure at least one address mapping set! Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 21.3 Configuring the PPTP Client



**The HomeSafe supports only one PPTP server connection at any given time.**

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= PPTP
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

```

**Figure 21-2 Internet Access Setup (PPTP)**

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

**Table 21-2 New Fields in Menu 4 (PPTP) Screen**

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>PPTP</b> . The encapsulation method influences your choices for the <b>IP Address</b> field.	<b>PPTP</b>
Idle Timeout	This value specifies the time, in seconds, that elapses before the HomeSafe automatically disconnects from the PPTP server.	<b>100 (default)</b>

## 21.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the appendix.

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= PPPoE
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

```

**Figure 21-3 Internet Access Setup (PPPoE)**

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

**Table 21-3 New Fields in Menu 4 (PPPoE) screen**

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>PPPoE</b> . The encapsulation method influences your choices in the <b>IP Address</b> field.	<b>PPPoE</b>

**Table 21-3 New Fields in Menu 4 (PPPoE) screen**

FIELD	DESCRIPTION	EXAMPLE
Idle Timeout	This value specifies the time in seconds that elapses before the HomeSafe automatically disconnects from the PPPoE server.	<b>100 (default)</b>

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

## 21.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your HomeSafe to operate on your network as well as access the Internet.



**When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.**

---

You may deactivate the firewall in menu 21.2 or via the HomeSafe embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

# Chapter 22

## Remote Node Configuration

*This chapter covers remote node configuration.*

### 22.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options**, **Menu 11.5 - Remote Node Filter** and **Menu 11.6 - Traffic Redirect Setup**.

### 22.2 Remote Node Profile Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Profile** (shown below).  
The following explains how to configure the remote node profile menu.

#### 22.2.1 Ethernet Encapsulation

There are two variations of menu 11 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP	Route= IP
Active= Yes	
Encapsulation= Ethernet	Apply Alias= None
Service Type= Standard	Edit IP= No
Service Name= N/A	Session Options:
Outgoing:	Edit Filter Sets= No
My Login= N/A	
My Password= N/A	Edit Traffic Redirect= No
Retype to Confirm= N/A	
Server= N/A	
Relogin Every (min)= N/A	

Press ENTER to Confirm or ESC to Cancel:

**Figure 22-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation**

The following table describes the fields in this menu.



**Table 22-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation**

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> (activate remote node) or <b>No</b> (deactivate remote node).	<b>Yes</b>
Encapsulation	<b>Ethernet</b> is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to <b>PPPoE</b> or <b>PPTP</b> encapsulation.	<b>Ethernet</b>
Service Type	Press [SPACE BAR] and then [ENTER] to select from <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method), <b>RR-Telstra</b> or <b>Telia Login</b> . Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .	<b>Standard</b>
Outgoing		
My Login	This field is applicable for <b>PPPoE</b> encapsulation only. Enter the login name assigned by your ISP when the HomeSafe calls this remote node. Some ISPs append this field to the <b>Service Name</b> field above (e.g., jim@poellc) to access the PPPoE server.	jim
My Password	Enter the password assigned by your ISP when the HomeSafe calls this remote node. Valid for <b>PPPoE</b> encapsulation only.	*****
Retype to Confirm	Type your password again to make sure that you have entered it correctly.	*****
Server	This field is valid only when <b>RoadRunner</b> is selected in the <b>Service Type</b> field. The HomeSafe will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Relogin Every (min)	This field is available when you select <b>Telia Login</b> in the <b>Service Type</b> field.  The Telia server logs the HomeSafe out if the HomeSafe does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the HomeSafe to wait between logins.	
Route IP	This field refers to the protocol that will be routed by your HomeSafe – IP is the only option for the HomeSafe.	<b>IP</b>
Apply Alias	Press [SPACE BAR] to choose <b>Alias 1</b> or <b>Alias 2</b> .  IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The HomeSafe supports three logical LAN interfaces via its single physical Ethernet interface with the HomeSafe itself as the gateway for each LAN network.	<b>Alias 1</b>
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to go to <b>Menu 11.3 - Remote Node Network Layer Options</b> .	<b>No</b> (default)
Session Options		
Edit Filter Sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	<b>No</b> (default)
Edit Traffic Redirect	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> .  Select <b>Yes</b> and press [ENTER] to configure <b>Menu 11.6 Traffic Redirect Setup</b> . Select <b>No</b> (default) if you do not want to configure this feature.	

**Table 22-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation**

FIELD	DESCRIPTION	EXAMPLE
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

### 22.2.2 PPPoE Encapsulation

The HomeSafe supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the HomeSafe with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see the appendix for more information on PPPoE.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes

Encapsulation= PPPoE                Apply Alias= None
Service Type= Standard              Edit IP= No
Service Name=                       Telco Option:
Outgoing:                           Allocated Budget(min)= 0
  My Login=                          Period(hr)= 0
  My Password= *****              Schedules=
  Retype to Confirm= *****        Nailed-Up Connection= No
  Authen= CHAP/PAP

Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= 100

Edit Traffic Redirect= No

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 22-2 Menu 11.1 Remote Node Profile for PPPoE Encapsulation**

### Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

### Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The HomeSafe does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the HomeSafe will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in *Table 22-1*.

**Table 22-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)**

FIELD	DESCRIPTION	EXAMPLE
Service Name	If you are using <b>PPPoE</b> encapsulation, then type the name of your PPPoE service here. Only valid with <b>PPPoE</b> encapsulation.	poellc
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <b>CHAP/PAP</b> - Your HomeSafe will accept either <b>CHAP</b> or <b>PAP</b> when requested by this remote node. <b>CHAP</b> - accept CHAP only. <b>PAP</b> - accept PAP only.	<b>CHAP/PAP</b>
Telco Option		
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the <b>Allocated Budget</b> is (10 minutes) and the <b>Period(hr)</b> is 1 (hour).	0 (default)
Schedules	You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	<b>No</b> (default)
Session Options		
Idle Timeout	Type the length of idle time (when there is no traffic from the HomeSafe to the remote node) in seconds that can elapse before the HomeSafe automatically disconnects the PPPoE connection. This option only applies when the HomeSafe initiates the call.	100 seconds (default)

### 22.2.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the appendix for information on PPTP.

```

Menu 11.1 - Remote Node Profile

Rem Node Name=                               Route=
Active=                                         Apply Alias=
Encapsulation=                               Edit IP=
Service Type=                               Telco Option:
Service Name= N/A                           Allocated Budget (min)=
Outgoing:                                   Period(hr)=
  My Login=                                 Schedules=
  My Password=                             Nailed-Up Connection=
  Retype to Confirm=
  Authen=
PPTP My IP:                                Session Options:
  My IP Addr=                              Edit Filter Sets=
  My IP Mask=                              Idle Timeout(sec)=
  Server IP Addr=                          Edit Traffic Redirect=
  Connection ID/Name=

Press ENTER to Confirm or ESC to Cancel:

```

The next table shows how to configure fields in menu 11.1 not previously discussed.

**Table 22-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation**

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select <b>PPTP</b> . You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	<b>PPTP</b>
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My IP Mask	Enter the subnet mask of the WAN Ethernet port.	255.255.255.0
Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP

## 22.3 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

**Figure 22-4 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation**

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

**Table 22-4 Remote Node Network Layer Options**

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> ; otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.	<b>Dynamic</b> (default)
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.	
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	This field is applicable to <b>Ethernet</b> encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.	

Table 22-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
My WAN Addr	This field is applicable to <b>PPPoE</b> and <b>PPTP</b> encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your HomeSafe. Note that this is the address assigned to your local HomeSafe, not the remote router.	
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose <b>None</b> to disable NAT. Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b> . Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b> , <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b> , <b>Many- One-to-One</b> and <b>Server</b> . When you select <b>Full Feature</b> you must configure at least one address mapping set! See the <i>NAT chapter</i> for a full discussion on this feature.	<b>SUA Only</b> (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the HomeSafe's routes (see the <i>Metric</i> section in the <i>WAN and Dial Backup Setup</i> chapter) The smaller the number, the higher priority the route has.	1
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the HomeSafe will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.	<b>No</b>
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from <b>Both/ None/In Only/Out Only</b> . See the <i>LAN Setup</i> chapter for more information on RIP. The default for RIP on the WAN side is <b>None</b> . It is recommended that you do not change this setting.	<b>None</b> (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> or <b>None</b> .	N/A
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The HomeSafe supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it. See the <i>LAN Setup</i> chapter for more information on this feature.	<b>None</b> (default)
Once you have completed filling in <b>Menu 11.3 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

## 22.4 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the HomeSafe to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to the Filters chapter. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

```

Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:

```

**Figure 22-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)**

```

Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:

```

**Figure 22-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)**

### 22.4.1 Traffic Redirect Setup

Configure parameters that determine when the HomeSafe will forward WAN traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.

```

Menu 11.6 - Traffic Redirect Setup

Active= Yes
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 14
  Check WAN IP Address= 0.0.0.0
  Fail Tolerance= 2
  Period(sec)= 5
  Timeout(sec)= 3

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 22-7 Menu 11.6: Traffic Redirect Setup**

The following table describes the fields in this screen.

Table 22-5 Menu 11.6: Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and select <b>Yes</b> (to enable) or <b>No</b> (to disable) traffic redirect setup. The default is <b>No</b> .	<b>Yes</b>
Configuration:		
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The HomeSafe automatically forwards traffic to this IP address if the HomeSafe's Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route's priority among the HomeSafe's routes (see the <i>Metric</i> section in the <i>WAN and Dial Backup Setup</i> chapter) The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your HomeSafe's WAN accessibility. The HomeSafe uses the default gateway IP address if you do not enter an IP address here.  If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the HomeSafe to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0
Fail Tolerance	Enter the number of times your HomeSafe may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the HomeSafe waits for a ping response from the IP Address in the <b>Check WAN IP Address</b> field before it times out. The number in this field should be less than the number in the <b>Period</b> field. Three to 50 is usually a good number.  The WAN connection is considered "down" after the HomeSafe times out the number of times specified in the <b>Fail Tolerance</b> field.	3
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

# Chapter 23

## Static Route Setup

*This chapter shows how to setup IP static routes.*

### 23.1 IP Static Route Setup

**Step 1.** To configure an IP static route, use **Menu 12 – Static Routing Setup** (shown next).

Menu 12 - IP Static Route Setup

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

7. \_\_\_\_\_

8. \_\_\_\_\_

Enter selection number:

**Figure 23-1 Menu 12 IP Static Route Setup**

**Step 2.** Now, type the route number of a static route you want to configure.

Menu 12.1 - Edit IP Static Route

Route #: 1

Route Name= ?

Active= No

Destination IP Address= ?

IP Subnet Mask= ?

Gateway IP Address= ?

Metric= 2

Private= No

- . -

**Figure 23-2 Menu12.1 Edit IP Static Route**

The following table describes the fields for **Menu 12.1 – Edit IP Static Route Setup**.

**Table 23-1 Menu12.1 Edit IP Static Route**

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.



**Table 23-1 Menu12.1 Edit IP Static Route**

FIELD	DESCRIPTION
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your HomeSafe that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your HomeSafe; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the HomeSafe will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and is not included in RIP broadcasts. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

# Chapter 24

## Dial-in User Setup

*This chapter shows you how to create user accounts on the HomeSafe.*

### 24.1 Dial-in User Setup

By storing user profiles locally, your HomeSafe is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your HomeSafe.

**Step 1.** From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

```

Menu 14 - Dial-in User Setup

1. _____ 9. _____ 17. _____ 25. _____
2. _____ 10. _____ 18. _____ 26. _____
3. _____ 11. _____ 19. _____ 27. _____
4. _____ 12. _____ 20. _____ 28. _____
5. _____ 13. _____ 21. _____ 29. _____
6. _____ 14. _____ 22. _____ 30. _____
7. _____ 15. _____ 23. _____ 31. _____
8. _____ 16. _____ 24. _____ 32. _____
    
```

**Figure 24-1 Menu 14- Dial-in User Setup**

**Step 2.** Type a number and press [ENTER] to edit the user profile.

```

Menu 14.1 - Edit Dial-in User

User Name= test
Active= Yes
Password= *****

Press ENTER to Confirm or ESC to Cancel:
    
```

**Figure 24-2 Menu 14.1- Edit Dial-in User**

The following table describes the fields in this screen.

**Table 24-1 Menu 14.1- Edit Dial-in User**

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	



# Chapter 25

## Network Address Translation (NAT)

*This chapter discusses how to configure NAT on the HomeSafe.*

### 25.1 Using NAT



**You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the HomeSafe.**

#### 25.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section 25.3.1* for a detailed description of the NAT set for SUA. The HomeSafe also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.



**Choose SUA Only if you have just one public WAN IP address for your HomeSafe.**



**Choose Full Feature if you have multiple public WAN IP addresses for your HomeSafe.**

### 25.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only
  
```

**Figure 25-1 Menu 4 Applying NAT for Internet Access**

The following figure shows how you apply NAT to the remote node in menu 11.1.

**Step 1.** Enter 11 from the main menu.

**Step 2.** When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

**Step 3.** Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
Version= N/A
Multicast= None
```

**Figure 25-2 Menu 11.3 Applying NAT to the Remote Node**

The following table describes the options for Network Address Translation.

**Table 25-1 Applying NAT in Menus 4 & 11.3**

FIELD	DESCRIPTION	EXAMPLE
NAT	Press [SPACE BAR] and then [ENTER] to select <b>Full Feature</b> if you have multiple public WAN IP addresses for your HomeSafe. The SMT uses the address mapping set that you configure and enter in the <b>Address Mapping Set</b> field (menu 15.1 - see section 25.3.1).	<b>Full Feature</b>
	Select <b>None</b> to disable NAT.	<b>None</b>
	When you select <b>SUA Only</b> , the SMT uses Address Mapping Set 255 (menu 15.1 - see section 25.3.1). Choose <b>SUA Only</b> if you have just one public WAN IP address for your HomeSafe.	<b>SUA Only</b>

**25.3 NAT Setup**

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
Menu 15 - NAT Setup

1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup
```

**Figure 25-3 Menu 15 NAT Setup**

### 25.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

```

Menu 15.1 - Address Mapping Sets

1. NAT_SET
255. SUA (read only)
  
```

**Figure 25-4 Menu 15.1 Address Mapping Sets**

#### SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 25.1.1*). The fields in this menu cannot be changed.

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   0.0.0.0        255.255.255.255  0.0.0.0          M-1
2.                                     0.0.0.0          Server
3.
4.
5.
6.
7.
8.
9.
10.
  
```

**Figure 25-5 Menu 15.1.255 SUA Address Mapping Rules**

The following table explains the fields in this menu.

---

 **Menu 15.1.255 is read-only.**

---

**Table 25-2 SUA Address Mapping Rules**

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	<b>Local Start IP</b> is the starting local IP address (ILA).	0.0.0.0
Local End IP	<b>Local End IP</b> is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global Start IP</b> .	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	

Table 25-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Type	These are the mapping types. <b>Server</b> allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

### User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx  Local Start IP   Local End IP       Global Start IP   Global End IP
Type
----
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

```

Figure 25-6 Menu 15.1.1 First Set



If the Set Name field is left blank, the entire set will be deleted.



The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

### Ordering Your Rules

Ordering your rules is important because the HomeSafe applies the rules in the order that you specify. When a rule matches the current packet, the HomeSafe takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 25-3 Menu 15.1.1 First Set

FIELD	DESCRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is <b>Edit</b> . <b>Edit</b> means you want to edit a selected rule (see following field). <b>Insert Before</b> means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. <b>Delete</b> means to delete the selected rule and then all the rules after the selected one will be advanced one rule. <b>None</b> disables the <b>Select Rule</b> item.	<b>Edit</b>
Select Rule	When you choose <b>Edit</b> , <b>Insert Before</b> or <b>Delete</b> in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1



**You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.**

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.



**An End IP address must be numerically greater than its corresponding IP Start address.**

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 0.0.0.0
  End   = N/A

Global IP:
  Start= 0.0.0.0
  End   = N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 25-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

The following table explains the fields in this menu.

Table 25-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. <b>Server</b> allows you to specify multiple servers of different types behind NAT to this computer. See <i>section 25.5.3</i> for an example.	<b>One-to-One</b>
Local IP	Only local IP fields are <b>N/A</b> for server; Global IP fields <b>MUST</b> be set for	



**Table 25-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set**

FIELD	DESCRIPTION	EXAMPLE
	<b>Server.</b>	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is <b>N/A</b> for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global IP Start</b> . Note that <b>Global IP Start</b> can be set to 0.0.0.0 only if the types are <b>Many-to-One</b> or <b>Server</b> .	0.0.0.0
End	This is the ending inside global IP address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> types.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

## 25.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

**Step 1.** Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.

**Step 2.** Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
-----	-----	-----	-----
1.	Default	Default	0.0.0.0
2.	21	25	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0
Press ENTER to Confirm or ESC to Cancel:			

**Figure 25-8 Menu 15.2.1 NAT Server Setup**

**Step 3.** Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

**Step 4.** Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

**Step 5.** Press [ENTER] at the "Press ENTER to confirm ..." prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

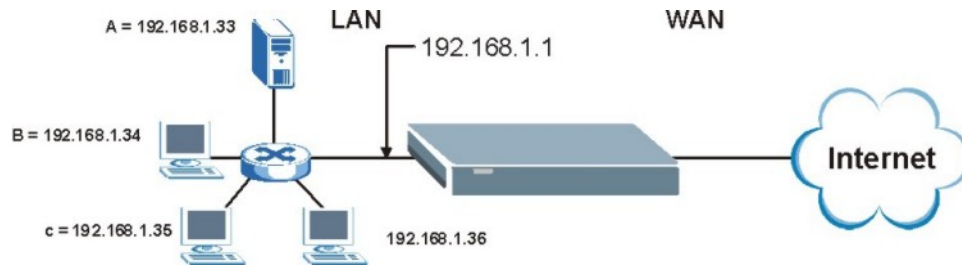


Figure 25-9 Multiple Servers Behind NAT Example

## 25.5 General NAT Examples

The following are some examples of NAT configuration.

### 25.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where the ILAs (Inside Local Addresses) of computers A through D map to one dynamic IGA (Inside Global Address) assigned by your ISP.

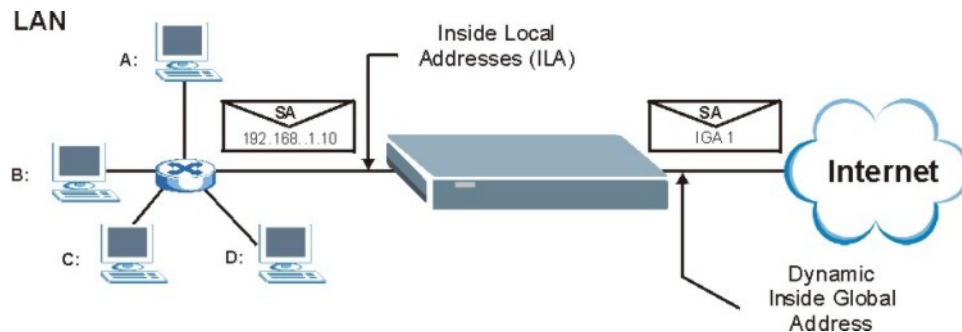


Figure 25-10 NAT Example 1

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only
  
```

Figure 25-11 Menu 4 Internet Access &amp; NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 25.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

### 25.5.2 Example 2: Internet Access with an Inside Server

The dynamic Inside Global Address is assigned by the ISP.

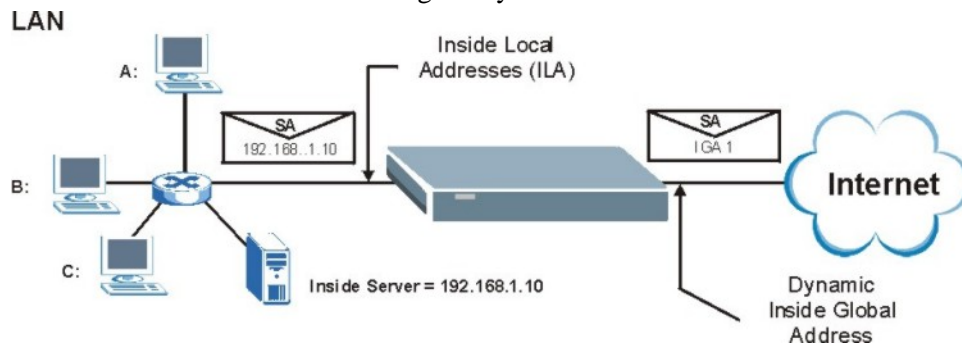


Figure 25-12 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

Menu 15.2.1 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Figure 25-13 Menu 15.2.1 Specifying an Inside Server

### 25.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

- Rule 1.** Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 2.** Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 3.** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- Rule 4.** You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

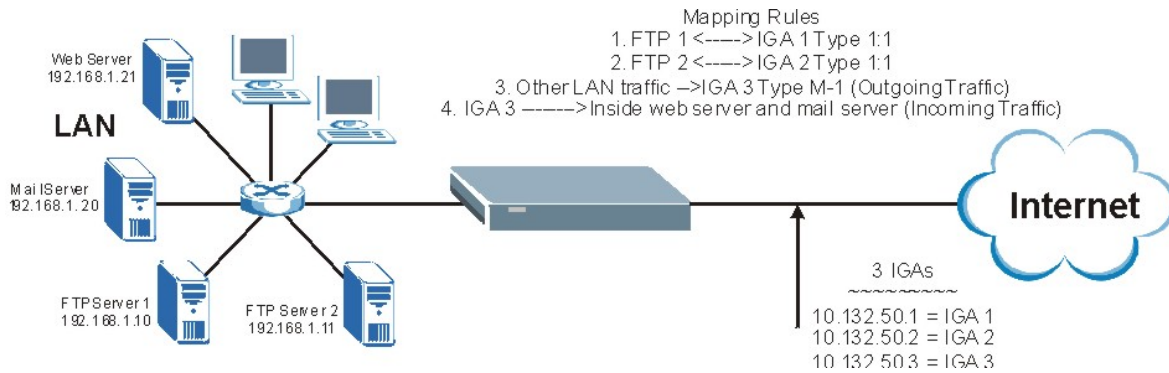


Figure 25-14 NAT Example 3

- Step 1.** In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in
- Step 2.** *Figure 25-15.*
- Step 3.** Then enter 15 from the main menu.
- Step 4.** Enter 1 to configure the Address Mapping Sets.
- Step 5.** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- Step 6.** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See
- Step 7.** *Figure 25-16.*
- Step 8.** Repeat the previous step for rules 2 to 4 as outlined above.
- Step 9.** When finished, menu 15.1.1.1 should look like as shown in *Figure 25-17.*

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= 1
Private= N/A
RIP Direction= None
Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 25-15 Example 3: Menu 11.3

The following figures show how to configure the first rule.

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 192.168.1.10
  End  = N/A

Global IP:
  Start= 10.132.50.1
  End  = N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 25-16 Example 3: Menu 15.1.1.1

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
-----
1.   192.168.1.10      10.132.50.1    1-1
2.   192.168.1.11      10.132.50.2    1-1
3.   0.0.0.0           255.255.255.255 10.132.50.3     M-1
4.                                     10.132.50.3     Server
5.
6.
7.
8.
9.
10.

Action= None      Select Rule= N/A

```

Figure 25-17 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

**Step 10.** Enter 15 from the main menu.

**Step 11.** Enter 2 in **Menu 15 - NAT Setup**.

**Step 12.** Enter 1 in **Menu 15.2 - NAT Server Setup** to see the following menu. Configure it as shown.

```

Menu 15.2 - NAT Server Setup

Rule  Start Port No.  End Port No.  IP Address
-----
1.   Default         Default       0.0.0.0
2.   80              80           192.168.1.21
3.   25              25           192.168.1.20
4.   0               0            0.0.0.0
5.   0               0            0.0.0.0
6.   0               0            0.0.0.0
7.   0               0            0.0.0.0
8.   0               0            0.0.0.0
9.   0               0            0.0.0.0
10.  0               0            0.0.0.0
11.  0               0            0.0.0.0
12.  0               0            0.0.0.0

```

## Example 3: Menu 15.2

**25.5.4 Example 4: NAT Unfriendly Application Programs**

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

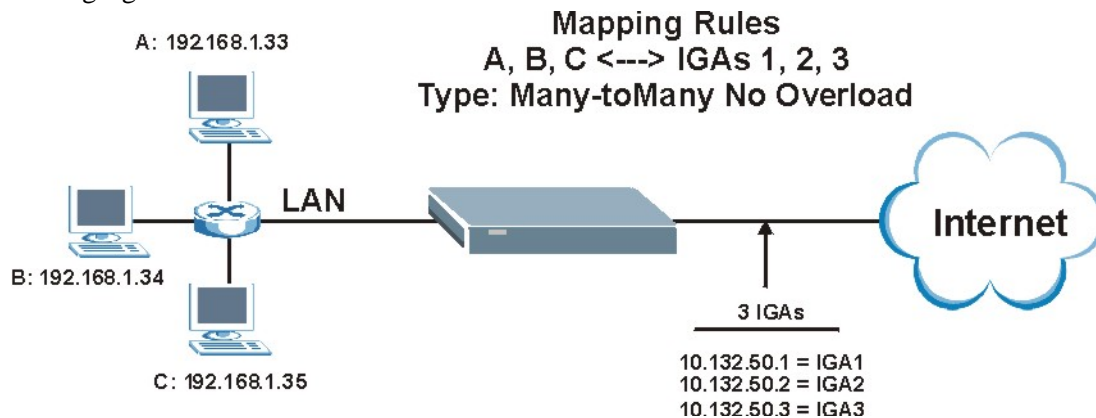


Figure 25-18 NAT Example 4



**Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One and Many-to-Many No Overload mapping types.**

Follow the steps outlined in example 3 to configure these two menus as follows.

```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:

```

Figure 25-19 Example 4: Menu 15.1.1.1 Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example4

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   192.168.1.10   192.168.1.12  10.132.50.1     10.132.50.3   M:M NO OV
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```

Figure 25-20 Example 4: Menu 15.1.1 Address Mapping Rules

## 25.6 Configuring Trigger Port Forwarding



**Only one LAN computer can use a trigger port (range) at a time.**

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

```

Menu 15.3 - Trigger Port Setup

Rule      Name      Incoming      Trigger
Start Port End Port Start Port End Port
-----
1.   Real Audio   6970        7170        7070        7070
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Press ENTER to Confirm or ESC to Cancel:

```

Figure 25-21 Menu 15.3 Trigger Port Setup

The following table describes the fields in this screen.

**Table 25-5 Menu 15.3 Trigger Port Setup**

<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The HomeSafe forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the HomeSafe to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		





# Chapter 26

## Enabling the Firewall

*This chapter shows you how to get started with the HomeSafe firewall.*

### 26.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

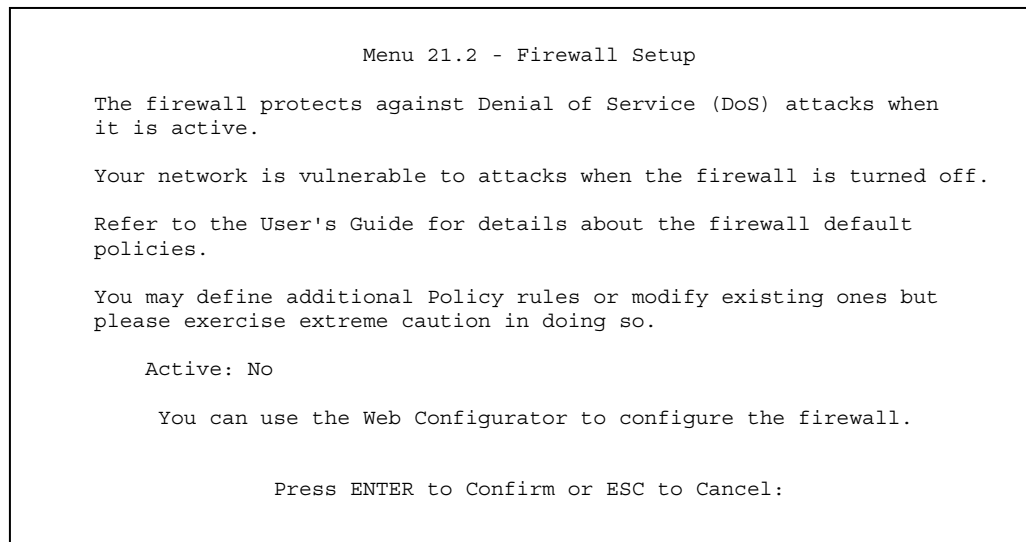
### 26.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your HomeSafe has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

### 26.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter and Firewall Setup** to display the screen shown next.

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.



**Figure 26-1 Menu 21.2 Firewall Setup**

Use the web configurator or the command interpreter to configure the firewall rules.

---

# Part VIII:

---

## SMT Advanced Management

---

This part discusses filtering setup, SNMP, system security, system information and diagnosis, firmware and configuration file maintenance, system maintenance, remote management and call scheduling.



**See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.**

---

# Chapter 27

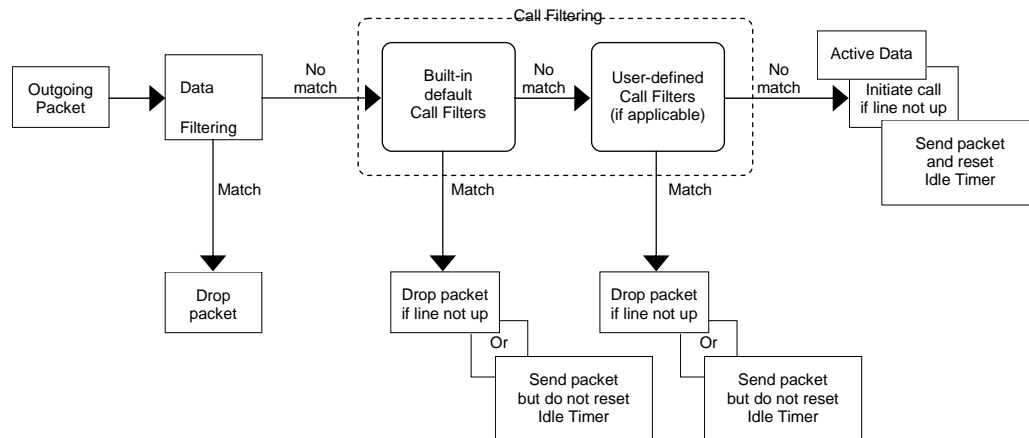
## Filter Configuration

*This chapter shows you how to create and apply filters.*

### 27.1 Introduction to Filters

Your HomeSafe uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.



**Figure 27-1 Outgoing Packet Filtering Process**

For incoming packets, your HomeSafe applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

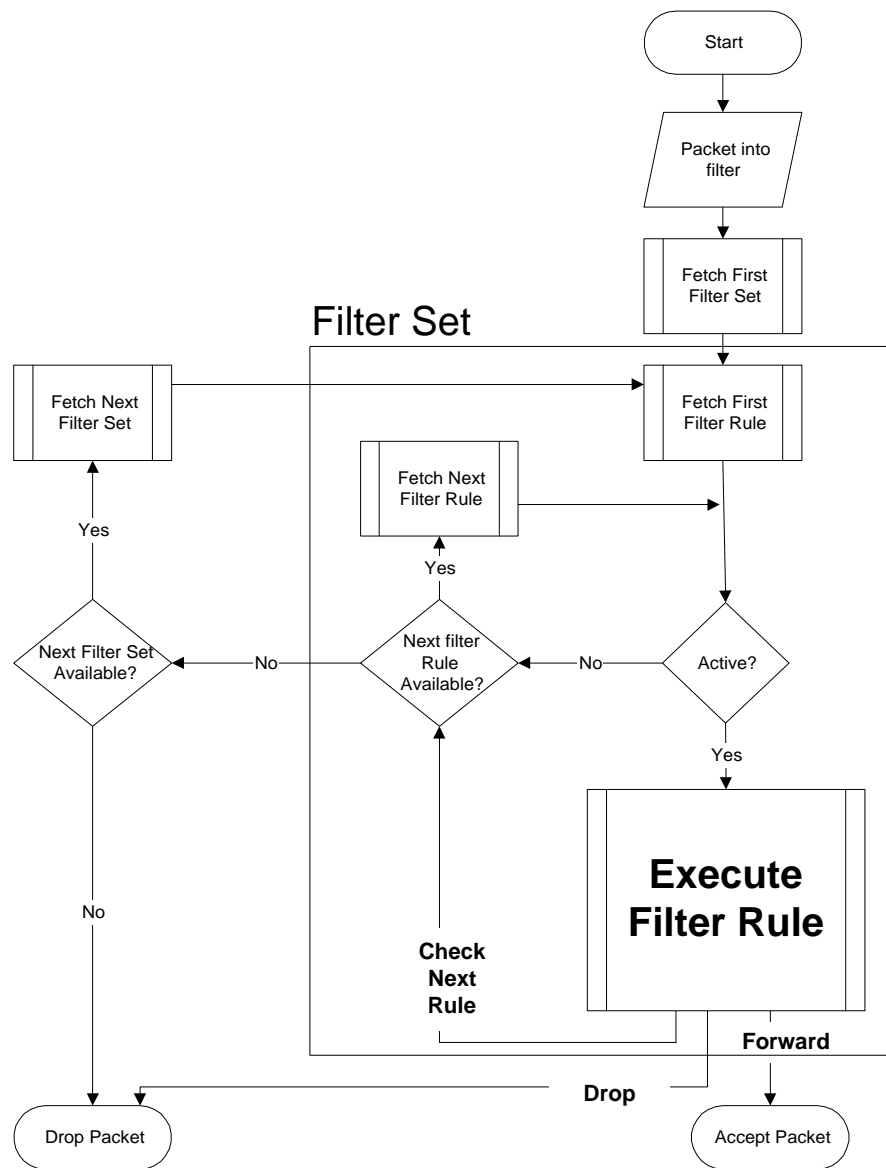
#### 27.1.1 The Filter Structure of the HomeSafe

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The HomeSafe allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can

apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also *Figure 27-7* for the logic flow when executing an IP filter.



**Figure 27-2 Filter Rule Process**

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## 27.2 Configuring a Filter Set

The HomeSafe includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

**Step 1.** Enter 21 in the main menu to open menu 21.

```

Menu 21 - Filter and Firewall Setup

      1. Filter Setup
      2. Firewall Setup

Enter Menu Selection Number:
  
```

**Figure 27-4 Menu 21: Filter and Firewall Setup**

**Step 2.** Enter 1 to bring up the following menu.

```

Menu 21.1 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
      1      _____      7      _____
      2      _____      8      _____
      3      _____      9      _____
      4      _____     10      _____
      5      _____     11      _____
      6      _____     12      _____

Enter Filter Set Number to Configure= 0
Edit Comments= N/A
Press ENTER to Confirm or ESC to Cancel:
  
```

**Figure 27-5 Menu 21.1: Filter Set Configuration**

**Step 3.** Select the filter set you wish to configure (1-12) and press [ENTER].

**Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

**Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

**Table 27-1 Abbreviations Used in the Filter Rules Summary Menu**

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.

**Table 27-1 Abbreviations Used in the Filter Rules Summary Menu**

FIELD	DESCRIPTION
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

**Table 27-2 Rule Abbreviations Used**

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

### 27.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the HomeSafe will warn you and will not allow you to save.

### 27.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port # = 137
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port # =
        Port # Comp= None
TCP Estab= N/A
More= No      Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 27-6 Menu 21.1.1.1 TCP/IP Filter Rule**

The following table describes how to configure your TCP/IP filter rule.

**Table 27-3 TCP/IP Filter Rule**

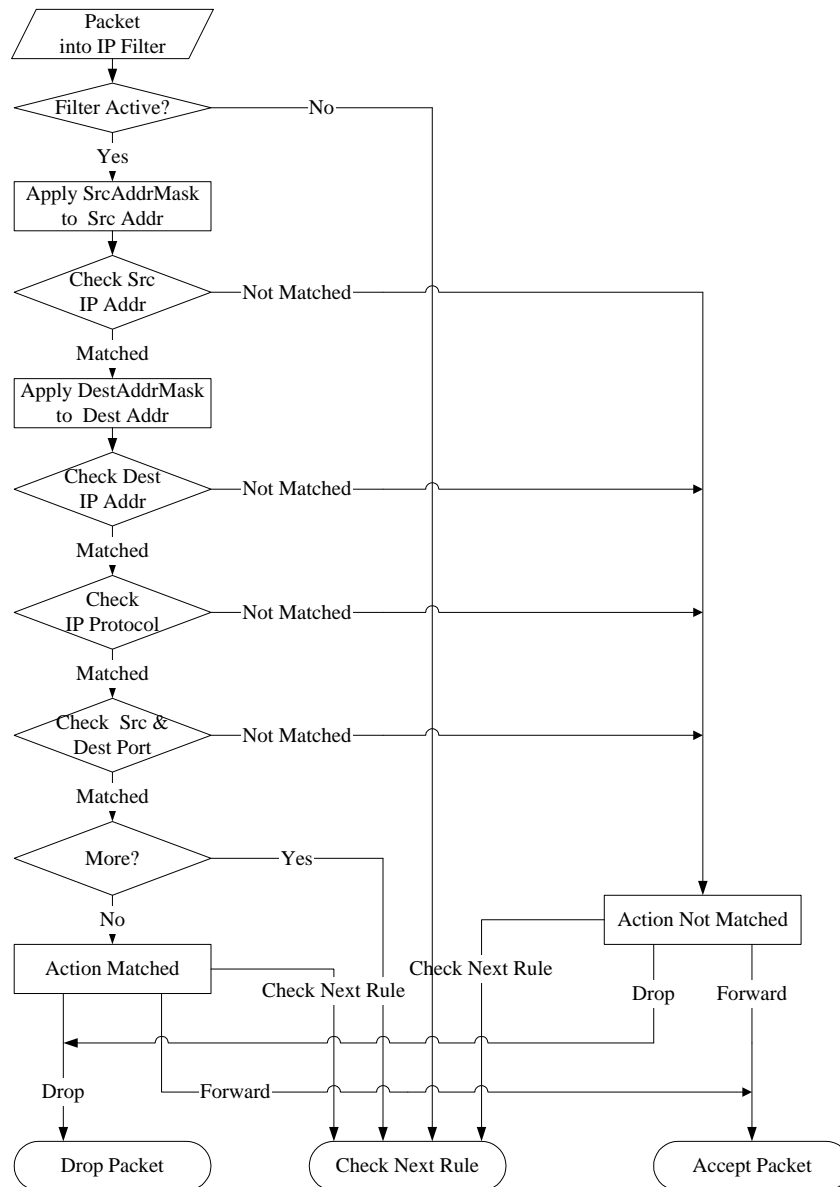
FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate the filter rule or <b>No</b> to deactivate it.	<b>Yes</b> <b>No</b>
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	<b>Yes</b> <b>No</b>
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the <b>Destination: IP Addr.</b>	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in <b>Destination: Port #.</b>	<b>None</b> <b>Less</b> <b>Greater</b> <b>Equal</b> <b>Not Equal</b>
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the <b>Source: IP Addr.</b>	0.0.0.0



Table 27-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in <b>Source: Port #</b> .	<b>None</b> <b>Less</b> <b>Greater</b> <b>Equal</b> <b>Not Equal</b>
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if <b>No</b> , it is ignored.	<b>Yes</b> <b>No</b>
More	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; if <b>No</b> , the packet is disposed of according to the action fields.  If <b>More</b> is <b>Yes</b> , then <b>Action Matched</b> and <b>Action Not Matched</b> will be <b>N/A</b> .	<b>Yes</b> <b>No</b>
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: <b>None</b> – No packets will be logged. <b>Action Matched</b> - Only packets that match the rule parameters will be logged. <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> – All packets will be logged.	<b>None</b> <b>Action Matched</b> <b>Action Not Matched</b> <b>Both</b>
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	<b>Check Next Rule</b> <b>Forward</b> <b>Drop</b>
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	<b>Check Next Rule</b> <b>Forward</b> <b>Drop</b>
When you have <b>Menu 21.1.1.1 - TCP/IP Filter Rule</b> configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.1 - Filter Rules Summary</b> .		

The following figure illustrates the logic flow of an IP filter.



### Figure 27-7 Executing an IP Filter

### 27.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the HomeSafe treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The HomeSafe applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

```

Menu 21.1.4.1 - Generic Filter Rule

Filter #: 4,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 27-8 Menu 21.1.4.1 Generic Filter Rule**

The following table describes the fields in the Generic Filter Rule menu.

**Table 27-4 Generic Filter Rule Menu Fields**

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	<b>Generic Filter Rule</b> <b>TCP/IP Filter Rule</b>
Active	Select <b>Yes</b> to turn on the filter rule or <b>No</b> to turn it off.	<b>Yes / No</b>
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If <b>More</b> is <b>Yes</b> , then Action Matched and Action Not Matched will be <b>No</b> .	<b>Yes</b> <b>No</b>
Log	Select the logging option from the following: <b>None</b> - No packets will be logged. <b>Action Matched</b> - Only packets that match the rule parameters will be logged. <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> - All packets will be logged.	<b>None</b> <b>Action Matched</b> <b>Action Not Matched</b> <b>Both</b>
Action Matched	Select the action for a packet matching the rule.	<b>Check Next Rule</b> <b>Forward</b> <b>Drop</b>

Table 27-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop
Once you have completed filling in <b>Menu 21.4.1.1 - Generic Filter Rule</b> , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.1 - Filter Rules Summary</b> .		

## 27.3 Example Filter

Let's look at an example to block outside users from accessing the HomeSafe via telnet.

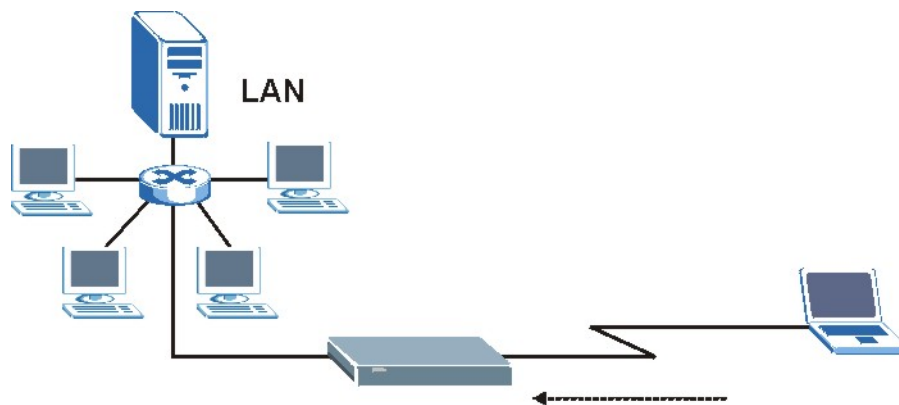


Figure 27-9 Telnet Filter Example

- Step 1.** Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- Step 2.** Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- Step 3.** Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

**Step 6.** Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1  
Filter Type= TCP/IP Filter Rule  
Active= Yes  
IP Protocol= 6  
Destination: IP Addr= 0.0.0.0  
IP Mask= 0.0.0.0  
Port # = 23  
Port # Comp= Equal  
Source: IP Addr= 0.0.0.0  
IP Mask= 0.0.0.0  
Port # = 0  
Port # Comp= None  
TCP Estab= No  
More= No  
Log= None  
Action Matched= Drop  
Action Not Matched= Forward  
Press ENTER to Confirm or ESC to Cancel:  
Press Space Bar to Toggle.

Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

**6** is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

There are no more rules to check.

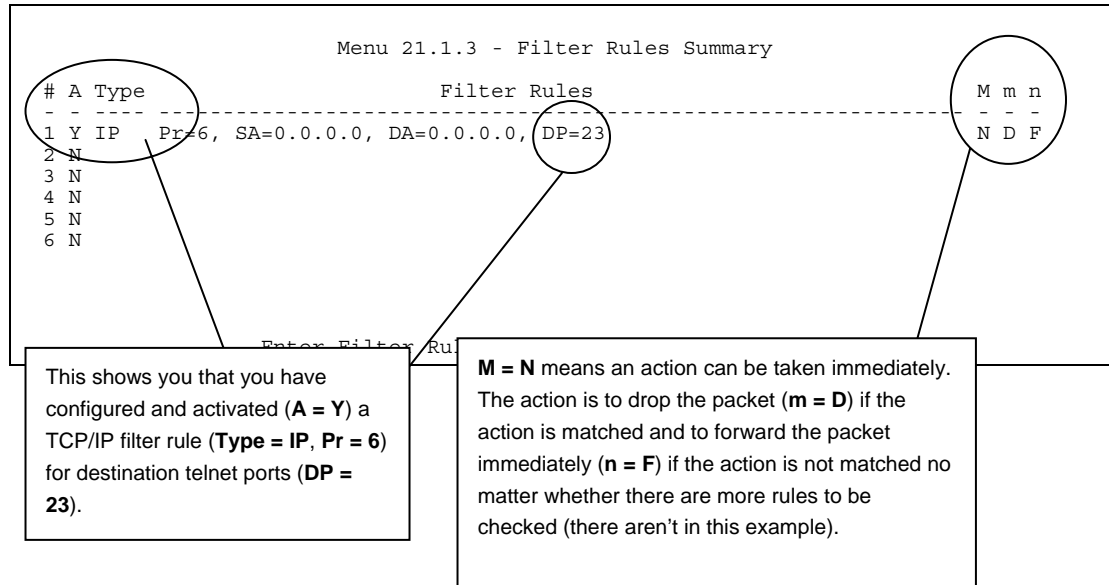
Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Equal** here as you are looking for packets going to port 23 only.

Select Forward here so that the packet will be forwarded if its destination is not the telnet port.

**Figure 27-10 Example Filter: Menu 21.1.3.1**

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.



**Figure 27-11 Example Filter Rules Summary: Menu 21.1.3**

After you've created the filter set, you must apply it.

- Step 1.** Enter 11 from the main menu to go to menu 11.
- Step 2.** Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- Step 3.** This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 27-14*.
- Step 4.** Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

## 27.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the HomeSafe applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the HomeSafe is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

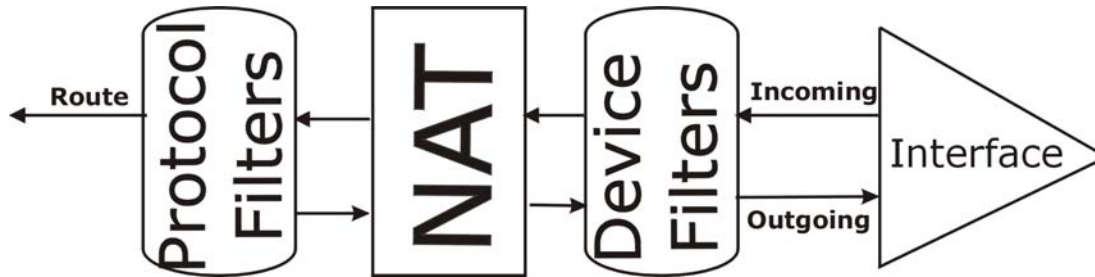


Figure 27-12 Protocol and Device Filter Sets

## 27.5 Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

## 27.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The HomeSafe already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.



**If you do not activate the firewall, it is advisable to apply filters.**

---

### 27.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the HomeSafe and output filter sets filter outgoing traffic from the HomeSafe. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

```
Menu 3.1 - LAN Port Filter Setup
Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Press ENTER to Confirm or ESC to Cancel:
```

Figure 27-13 Filtering LAN Traffic

### 27.6.2 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to

four filter sets by entering their numbers separated by commas. The HomeSafe already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 27-14 Filtering Remote Node Traffic**





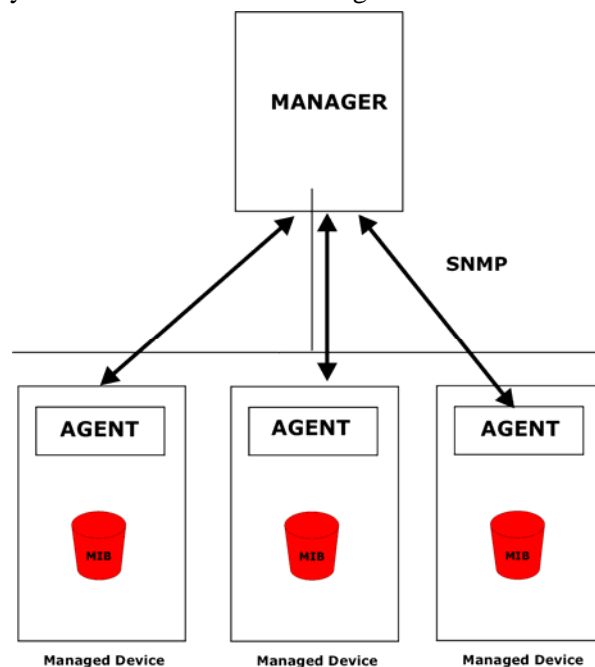
# Chapter 28

## SNMP Configuration

*This chapter explains SNMP Configuration menu 22.*

### 28.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your HomeSafe supports SNMP agent functionality, which allows a manager station to manage and monitor the HomeSafe through the network. The HomeSafe supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.



**Figure 28-1 SNMP Management Model**

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the HomeSafe). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include the number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.

- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## 28.2 Supported MIBs

The HomeSafe supports RFC-1215 and MIB II as defined in RFC-1213 as well as ZyXEL private MIBs. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

## 28.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

```
Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0
```

**Figure 28-2 Menu 22 SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 28-1 Menu 22 SNMP Configuration**

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the <b>Get Community</b> , which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the <b>Set</b> community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your HomeSafe will only respond to SNMP messages from this address. A blank (default) field means your HomeSafe will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

## 28.4 SNMP Traps

The HomeSafe will send traps to the SNMP manager when any one of the following events occurs:

**Table 28-2 SNMP Traps**

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart ( <i>defined in RFC-1215</i> )	A trap is sent after booting (power on).
2	warmStart ( <i>defined in RFC-1215</i> )	A trap is sent after booting (software reboot).
3	linkDown ( <i>defined in RFC-1215</i> )	A trap is sent with the port number when any of the links are down. See the following table.
4	linkUp ( <i>defined in RFC-1215</i> )	A trap is sent with the port number.
5	authenticationFailure ( <i>defined in RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP gets or sets requirements with wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).

The port number is its interface index under the interface group.

**Table 28-3 Ports and Permanent Virtual Circuits**

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
...	...
13	12
14	xDSL



# Chapter 29

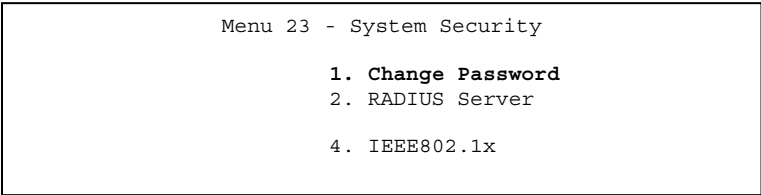
## System Security

*This chapter describes how to configure the system security on the HomeSafe.*

### 29.1 System Security

You can configure the system password, an external RADIUS server and 802.1x in this menu.

#### 29.1.1 System Password

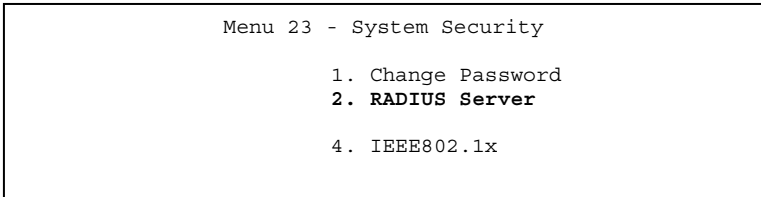


**Figure 29-1 Menu 23 System Security**

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the HomeSafe in the *Introducing the Web Configurator* chapter.

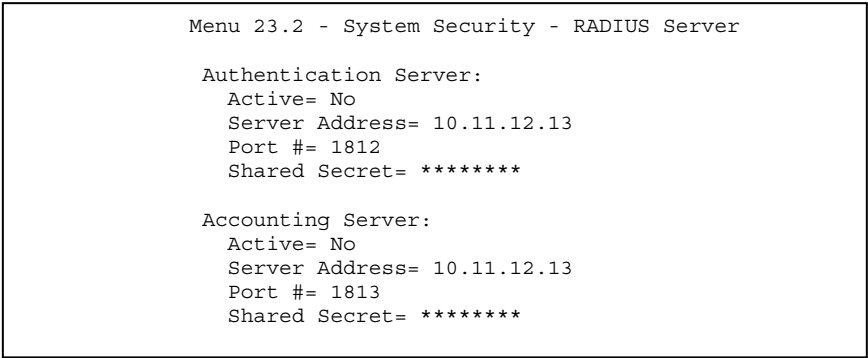
#### 29.1.2 Configuring External RADIUS Server

Enter 23 in the main menu to display **Menu 23 – System Security**.



**Figure 29-2 Menu 23 System Security**

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIUS Server** as shown next.



**Figure 29-3 Menu 23.2 System Security : RADIUS Server**

The following table describes the fields in this screen.

**Table 29-1 Menu 23.2 System Security : RADIUS Server**

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable user authentication through an external authentication server.	<b>No</b>
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.	10.11.12.13
Port	The default port of the RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.	<b>1812</b>
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and HomeSafe.	
Accounting Server		
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable user authentication through an external accounting server.	<b>No</b>
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13
Port	The default port of the RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.	<b>1813</b>
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and HomeSafe.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

### 29.1.3 802.1x

The IEEE802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your HomeSafe.

**Step 1.** From the main menu, enter 23 to display **Menu23 – System Security**.

Menu 23 - System Security
1. Change Password
2. RADIUS Server
4. IEEE802.1x

**Figure 29-4 Menu 23 System Security**

**Step 2.** Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

```

Menu 23.4 - System Security - IEEE802.1x

Wireless Port Control= No Authentication Required
ReAuthentication Timer (in second)= N/A
Idle Timeout (in second)= N/A

Key Management Protocol= N/A
Dynamic WEP Key Exchange= N/A
PSK = N/A
WPA Mixed Mode= N/A
Data Privacy = N/A
WPA Broadcast/Multicast Key Update Timer= N/A

Authentication Databases= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

**Figure 29-5 Menu 23.4 System Security : IEEE802.1x**

The following table describes the fields in this menu.

**Table 29-2 Menu 23.4 System Security : IEEE802.1x**

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access. Select <b>No Authentication Required</b> to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Selecting <b>Authentication Required</b> means wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select <b>No Access Allowed</b> to block all wireless stations access to the wired network. The following fields are not available when you select <b>No Authentication Required</b> or <b>No Access Allowed</b> .
ReAuthentica- tion Timer (in second)	Specify how often a client has to re-enter username and password to stay connected to the wired network. This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is <b>1800</b> seconds (or 30 minutes).
Idle Timeout (in second)	The HomeSafe automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. The default time interval is <b>3600</b> seconds (or 1 hour).
Key Management Protocol	Press [SPACE BAR] to select <b>802.1x</b> , <b>WPA</b> or <b>WPA-PSK</b> and press [ENTER].
Dynamic WEP Key Exchange	This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Also set the <b>Authentication Databases</b> field to <b>RADIUS Only</b> . Local user database may not be used. Select <b>Disable</b> to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption. Up to 32 stations can access the HomeSafe when you configure Dynamic WEP Key Exchange.



Table 29-2 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select <b>WPA-PSK</b> in the <b>Key Management Protocol</b> field.
WPA Mixed Mode	Select <b>Enable</b> to activate WPA mixed mode. Otherwise, select <b>Disable</b> and configure <b>Group Data Privacy</b> field.
Data Privacy for Broadcast/Multicast packets	<b>Group Data Privacy</b> allows you to choose <b>TKIP</b> (recommended) or <b>WEP</b> for broadcast and multicast ("group") traffic if the <b>Key Management Protocol</b> is <b>WPA</b> and <b>WPA Mixed Mode</b> is disabled. <b>WEP</b> is used automatically if you have enabled <b>WPA Mixed Mode</b> . All unicast traffic is automatically encrypted by <b>TKIP</b> when <b>WPA</b> or <b>WPA-PSK Key Management Protocol</b> is selected.
WPA Broadcast/Multicast Key Update Timer	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in WPA-PSK mode. The HomeSafe default is 1800 seconds (30 minutes).
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the HomeSafe. The RADIUS is an external server. Use this field to decide which database the HomeSafe should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. When you configure <b>Key Management Protocol</b> to <b>WPA</b> , the <b>Authentication Databases</b> must be <b>RADIUS Only</b> . You can only use the <b>Local User Database</b> with <b>802.1x Key Management Protocol</b> . Select <b>Local User Database Only</b> to have the HomeSafe just check the built-in user database on the HomeSafe for a wireless station's username and password. Select <b>RADIUS Only</b> to have the HomeSafe just check the user database on the specified RADIUS server for a wireless station's username and password. Select <b>Local first, then RADIUS</b> to have the HomeSafe first check the user database on the HomeSafe for a wireless station's username and password. If the user name is not found, the HomeSafe then checks the user database on the specified RADIUS server. Select <b>RADIUS first, then Local</b> to have the HomeSafe first check the user database on the specified RADIUS server for a wireless station's username and password. If the HomeSafe cannot reach the RADIUS server, the HomeSafe then checks the local user database on the HomeSafe. When the user name is not found or password does not match in the RADIUS server, the HomeSafe will not check the local user database and the authentication fails.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the HomeSafe for authentication.

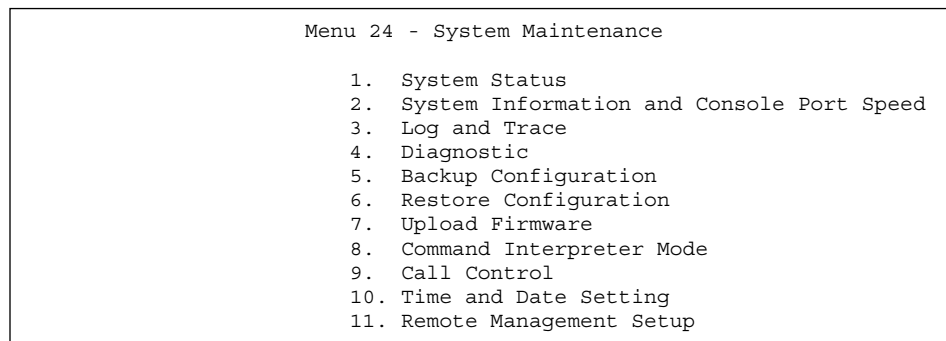
## Chapter 30

# System Information and Diagnosis

*This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.*

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.



**Figure 30-1 Menu 24 System Maintenance**

### 30.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next *Figure 30-2*. System Status is a tool that can be used to monitor your HomeSafe. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

Menu 24.1 - System Maintenance - Status					23:08:27		
					Sat. Jan. 01, 2000		
Port	Status	TxPkts	RxPkts	Cols	Tx B/s	Rx B/s	Up Time
WAN	Down	6	7038	0	0	0	0:00:00
LAN	100M/Full	9253	6154	0	0	0	23:08:26
WLAN	54M	3934	0	0	0	0	23:08:26
Port	Ethernet Address		IP Address		IP Mask		DHCP
WAN	00:50:8D:48:59:1F		172.21.3.125		255.255.0.0		Client
LAN	00:A0:C5:01:20:05		192.168.1.1		255.255.255.0		Server
WLAN	00:A0:C5:01:20:05						
System up Time:		23:08:31					
Name: HS-100W.zyxel.com.tw							
Routing: IP							
ZyNOS F/W Version: V3.60(JM.0)b1   05/17/2004							
Press Command:							
COMMANDS: 1-Drop WAN 9-Reset Counters ESC-Exit							

Figure 30-2 Menu 24.1 System Maintenance : Status

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 30-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	Identifies a port (WAN, LAN or WLAN) on the HomeSafe.
Status	Shows the port speed and duplex setting if you're using <b>Ethernet Encapsulation</b> and <b>Down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using <b>PPPoE Encapsulation</b> .
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the HomeSafe has been on.
Name	This is the HomeSafe's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

## 30.2 System Information

To get to the System Information:

**Step 1.** Enter 24 to display **Menu 24 — System Information and Console Port Speed**.

**Step 2.** Enter 2 to display **Menu 24.2 — System Information**.

**Step 3.** From this menu you have two choices as shown in the next figure:

```

Menu 24.2 - System Information and Console Port Speed
1. System Information
2. Console Port Speed

Please enter selection:

```

**Figure 30-3 Menu 24.2 System Information and Console Port Speed**

### 30.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```

Menu 24.2.1 - System Maintenance - Information

Name: HS-100W.zyxel.com.tw
Routing: IP
ZyNOS F/W Version: V3.60(JM.0)b1 | 05/17/2004
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:01:20:05
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

```

**Figure 30-4 Menu 24.2.1 System Maintenance : Information**

The following table describes the fields in this menu.

**Table 30-2 Menu 24.2.1 System Maintenance : Information**

FIELD	DESCRIPTION
Name	Displays the system name of your HomeSafe. This information can be changed in <b>Menu 1 – General Setup</b> .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your HomeSafe.
IP Address	This is the IP address of the HomeSafe in dotted decimal notation.
IP Mask	This shows the subnet mask of the HomeSafe.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the HomeSafe.

### 30.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your HomeSafe supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 30-5 Menu 24.2.2 System Maintenance : Change Console Port Speed**

## 30.3 Log and Trace

There are two logging facilities in the HomeSafe. The first is the error logs and trace records that are stored locally. The second is the syslog facility for message logging.

### 30.3.1 Syslog Logging

The HomeSafe uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance - Syslog Logging**, as shown next.

```
Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= 0.0.0.0
Log Facility= Local 1

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 30-6 Menu 24.3.2 System Maintenance : Syslog Logging**

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 30-3 Menu 24.3.2 System Maintenance : Syslog and Accounting**

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your HomeSafe sends five types of syslog messages. Some examples (not all HomeSafe specific) of these syslog messages with their message formats are shown next:

### 1. CDR

CDR Message Format
<pre>SdcmSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String ); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)       L02 Tunnel Connected(L2TP)       C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)       L02 Call Terminated       C02 Call Terminated Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated</pre>

### 2. Packet triggered

Packet triggered Message Format
<pre>SdcmSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String ); String = Packet trigger: Protocol=xx Data=xxxxxxxxxx...x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty-eight Hex characters to the server Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172 7374 Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000</pre>

### 3. Filter log

Filter log Message Format
<pre>SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String ); String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04&gt;R01mD IP[...] is the packet header and S04&gt;R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).       Src: Source Address       Dst: Destination Address       prot: Protocol ("TCP", "UDP", "ICMP")       spo: Source port       dpo: Destination port Mar 03 10:39:43 202.132.155.97 ZyXEL: GEN[fffffffffnordff0080] }S05&gt;R01mF Mar 03 10:41:29 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05&gt;R01mF Mar 03 10:41:34 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP] }S04&gt;R01mF Mar 03 11:59:20 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05&gt;R01mF Mar 03 12:00:52 202.132.155.97 ZyXEL: GEN[fffffffffff0080] }S05&gt;R01mF Mar 03 12:00:57 202.132.155.97 ZyXEL: GEN[00a0c5f502010080] }S05&gt;R01mF Mar 03 12:01:06 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021] }S04&gt;R01mF</pre>

### 4. PPP log

PPP Log Message Format
<pre>SdcmSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String ); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing</pre>

## 5. Firewall log

Firewall Log Message Format					
SdcmSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);					
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx   prot   rule   action]					
Src: Source Address					
spo: Source port (empty means no source port information)					
Dst: Destination Address					
dpo: Destination port (empty means no destination port information)					
prot: Protocol ("TCP", "UDP", "ICMP", "IGMP", "GRE", "ESP")					
rule: <a,b> where a means "set" number; b means "rule" number.					
Action: nothing(N) block (B) forward (F)					
08-01-2000	11:48:41	Local1.Notice	192.168.10.10	RAS: FW 172.21.1.80	:137 -
>172.21.1.80	:137	UDP default permit:<2,0> B			
08-01-2000	11:48:41	Local1.Notice	192.168.10.10	RAS: FW 192.168.77.88	:520 -
>192.168.77.88	:520	UDP default permit:<2,0> B			
08-01-2000	11:48:39	Local1.Notice	192.168.10.10	RAS: FW 172.21.1.50	->172.21.1.50
IGMP<2> default	permit:<2,0> B				
08-01-2000	11:48:39	Local1.Notice	192.168.10.10	RAS: FW 172.21.1.25	->172.21.1.25
IGMP<2> default	permit:<2,0> B				

### 30.3.2 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

IP Frame: ENET0-RECV Size: 44/ 44 Time: 17:02:44.262	
Frame Type:	
IP Header:	
IP Version	= 4
Header Length	= 20
Type of Service	= 0x00 (0)
Total Length	= 0x002C (44)
Identification	= 0x0002 (2)
Flags	= 0x00
Fragment Offset	= 0x00
Time to Live	= 0xFE (254)
Protocol	= 0x06 (TCP)
Header Checksum	= 0xFB20 (64288)
Source IP	= 0xC0A80101 (192.168.1.1)
Destination IP	= 0x00000000 (0.0.0.0)
TCP Header:	
Source Port	= 0x0401 (1025)
Destination Port	= 0x000D (13)
Sequence Number	= 0x05B8D000 (95997952)
Ack Number	= 0x00000000 (0)
Header Length	= 24
Flags	= 0x02 (...S.)
Window Size	= 0x2000 (8192)
Checksum	= 0xE06A (57450)
Urgent Ptr	= 0x0000 (0)
Options	=
0000: 02 04 02 00	
RAW DATA:	
0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01 E.....	
0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 .....	
0020: 60 02 20 00 E0 6A 00 00-02 04 02 00	
Press any key to continue...	

Figure 30-7 Call-Triggering Packet Example

## 30.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your HomeSafe to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to Diagnostic:

**Step 1.** From the main menu, type 24 to open **Menu 24 – System Maintenance**.

**Step 2.** From this menu, type 4 to open **Menu 24.4 – System Maintenance – Diagnostic**.

```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
  1. Ping Host
  2. WAN DHCP Release
  3. WAN DHCP Renewal
  4. Internet Setup Test

System
  11. Reboot System

Enter Menu Selection Number:

```

Figure 30-8 Menu 24.4 System Maintenance : Diagnostic

### 30.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 30-9*. LAN DHCP has already been discussed. The HomeSafe can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

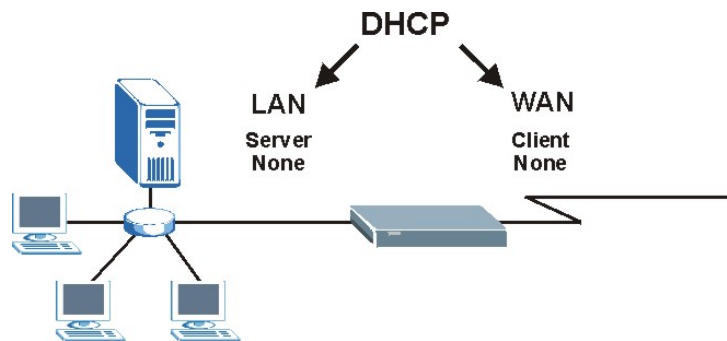


Figure 30-9 LAN &amp; WAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your HomeSafe and associated connections.

Table 30-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the <b>Host IP Address</b> field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in <b>Menu 4 - Internet Access</b> . Please refer to the <i>Internet Access</i> chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.



**Table 30-4 System Maintenance Menu Diagnostic**

Reboot System	Enter 11 to reboot the HomeSafe.
Host IP Address=	If you entered 1 in <b>Ping Host</b> , then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

# Chapter 31

## Firmware and Configuration File Maintenance

*This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.*

### 31.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the HomeSafe's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.



**Only use firmware for your HomeSafe's specific model.  
Refer to the label on the bottom of your HomeSafe.**

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the HomeSafe.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the HomeSafe only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the HomeSafe and the external filename refers to the filename not on the HomeSafe, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

**Table 31-1 Filename Conventions**

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the HomeSafe. Uploading the rom-0 file replaces the entire ROM file system, including your HomeSafe configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the HomeSafe.	*.bin

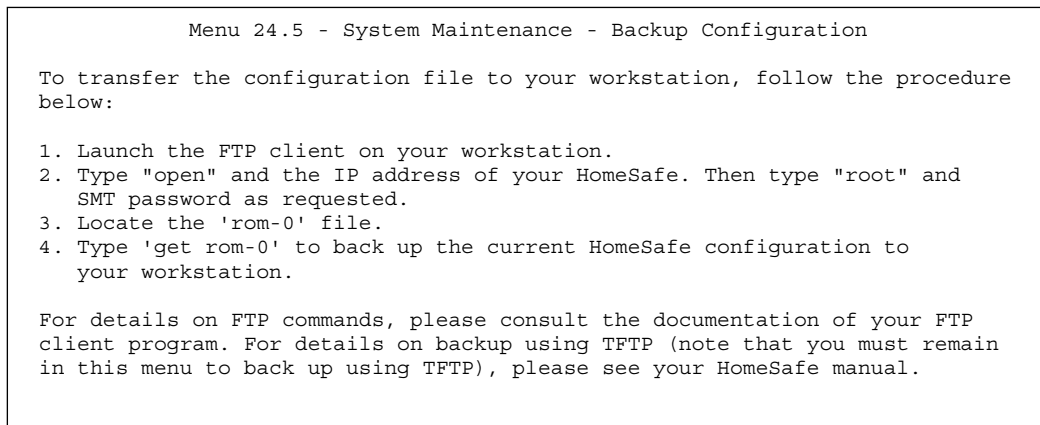
## 31.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current HomeSafe configuration to your computer. Backup is highly recommended once your HomeSafe is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the HomeSafe to the computer, while upload means from your computer to the HomeSafe.

### 31.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

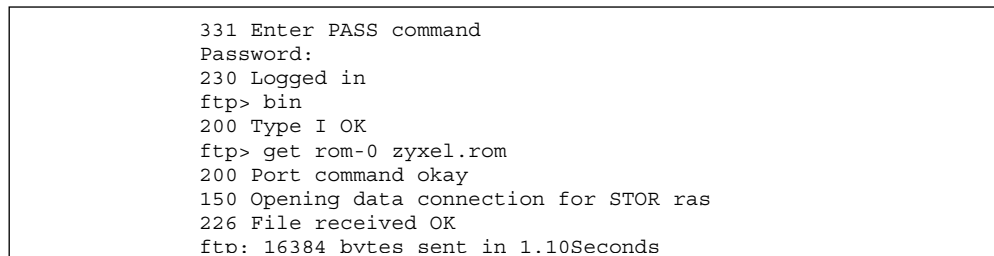


**Figure 31-1 Telnet in Menu 24.5**

### 31.2.2 Using the FTP Command from the Command Line

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your HomeSafe.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is “1234”).
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 6.** Use “get” to transfer files from the HomeSafe to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the HomeSafe to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter “quit” to exit the ftp prompt.

### 31.2.3 Example of FTP Commands from the Command Line



**Figure 31-2 FTP Session Example**

### 31.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 31-2 General Commands for GUI-based FTP Clients**

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

### 31.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
3. The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the HomeSafe will disconnect the Telnet session immediately.
4. You have an SMT console session running.

### 31.2.6 Backup Configuration Using TFTP

The HomeSafe supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

- Step 1.** Use telnet from your computer to connect to the HomeSafe and log in. Because TFTP does not have any security checks, the HomeSafe records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the HomeSafe. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the HomeSafe and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the HomeSafe to the computer and “binary” to set binary transfer mode.

### 31.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the HomeSafe IP address, “get” transfers the file source on the HomeSafe (rom-0, name of the configuration file on the HomeSafe) to the file destination on the computer and renames it config.rom.

### 31.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 31-3 General Commands for GUI-based TFTP Clients**

COMMAND	DESCRIPTION
Host	Enter the IP address of the HomeSafe. 192.168.1.1 is the HomeSafe's default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the HomeSafe and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the HomeSafe. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 31.2.5* to read about configurations that disallow TFTP and FTP over WAN.

## 31.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your HomeSafe since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.



#### **WARNING!**

**Do not interrupt the file transfer process as this may  
PERMANENTLY DAMAGE YOUR HomeSafe.**

---

### 31.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

## Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your HomeSafe. Then type "root" and SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of your backup configuration file on your workstation and rom-0 is the remote file name on the HomeSafe. This restores the configuration to your HomeSafe.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP client program. For details on backup using TFTP (note that you must remain in this menu to back up using TFTP), please see your HomeSafe manual.

**Figure 31-3 Telnet into Menu 24.6**

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open", followed by a space and the IP address of your HomeSafe.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is "1234").
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 6.** Find the "rom" file (on your computer) that you want to restore to your HomeSafe.
- Step 7.** Use "put" to transfer files from the HomeSafe to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the HomeSafe. See earlier in this chapter for more information on filename conventions.
- Step 8.** Enter "quit" to exit the ftp prompt. The HomeSafe will automatically restart after a successful restore process.

### 31.3.2 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

**Figure 31-4 Restore Using FTP Session Example**

Refer to *section 31.2.5* to read about configurations that disallow TFTP and FTP over WAN.

## 31.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.



**WARNING!**  
**DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR HOMESAFE.**

---

### 31.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the HomeSafe, you will see the following screens for uploading firmware and the configuration file using FTP.

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmware filename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your workstation and "ras" is the
   remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

**Figure 31-5 Telnet Into Menu 24.7.1 Upload System Firmware**

### 31.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put configuration filename rom-0" where "configurationfilename"
   is the name of your system configuration file on your workstation, which
   will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration
   file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

**Figure 31-6 Telnet Into Menu 24.7.2 System Maintenance**

To upload the firmware and the configuration file, follow these examples

### 31.4.3 FTP File Upload Command from the DOS Prompt Example

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your HomeSafe.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is “1234”).
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 6.** Use “put” to transfer files from the computer to the HomeSafe, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the HomeSafe and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the HomeSafe and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the HomeSafe to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter “quit” to exit the ftp prompt.



**The HomeSafe automatically restarts after a successful file upload.**

### 31.4.4 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftn: 1103936 bytes sent in 1.10Seconds
```

**Figure 31-7 FTP Session Example of Firmware File Upload**

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 31.2.5* to read about configurations that disallow TFTP and FTP over WAN.

### 31.4.5 TFTP File Upload

The HomeSafe also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- Step 1.** Use telnet from your computer to connect to the HomeSafe and log in. Because TFTP does not have any security checks, the HomeSafe records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the HomeSafe. Set the transfer mode to binary before starting data transfer.



**Step 5.** Use the TFTP client (see the example below) to transfer files between the HomeSafe and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the HomeSafe in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the HomeSafe to the computer, “put” the other way around, and “binary” to set binary transfer mode.

#### **31.4.6 TFTP Upload Command Example**

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the HomeSafe’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the HomeSafe).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

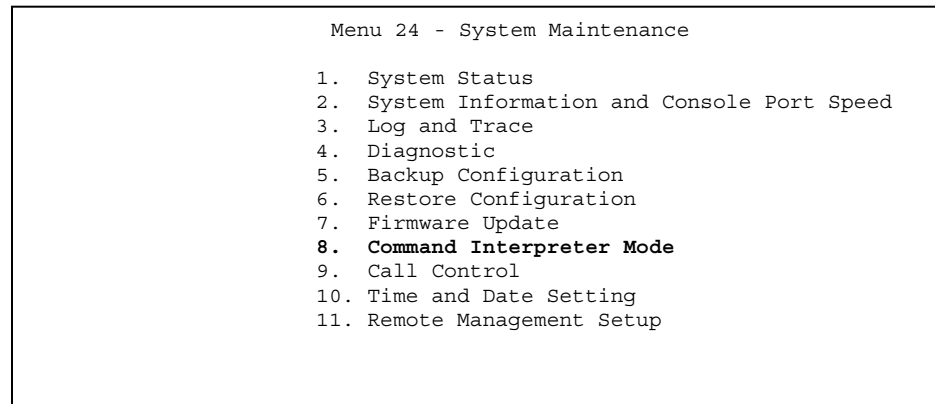
# Chapter 32

## System Maintenance

*This chapter leads you through SMT menus 24.8 to 24.10.*

### 32.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the [zyxel.com](http://zyxel.com) web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “`exit`” to return to the SMT main menu when finished.



**Figure 32-1 Command Mode in Menu 24**

#### 32.1.1 Command Syntax

The command keywords are in `courier` new font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets `<>`.

The optional fields in a command are enclosed in square brackets `[]`.

The `|` symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

#### 32.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

```
HS-100W> com
Valid commands are:
sys                exit                device        ether
poe                pptp                config        wlan
ip                 ppp                bridge        parentCtrl
radius             8021x
HS-100W>
```

**Figure 32-2 Valid Commands**

## 32.2 Call Control Support

The HomeSafe provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the HomeSafe within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management
2. Call History
```

**Figure 32-3 Menu 24.9 System Maintenance : Call Control**

### 32.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

```
Menu 24.9.1 - Budget Management

Remote Node      Connection Time/Total Budget  Elapsed Time/Total
1. MyISP         No Budget                    Period
                                      No Budget

Reset Node (0 to update screen):
```

**Figure 32-4 Budget Management**

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

**Table 32-1 Budget Management**

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

### 32.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Menu 24.9.2 - Call History						
Phone	Dir	Rate	#call	Max	Min	Total
Number						
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
Enter Entry to Delete(0 to exit):						

**Figure 32-5 Call History**

The following table describes the fields in this screen.

**Table 32-2 Call History Fields**

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or "0" to exit.	

## 32.3 Time and Date Setting

The Real Time Chip (RTC) keeps track of the time and date (not available on all models). There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your HomeSafe. Menu 24.10 allows you to update the time and date settings of your HomeSafe. The real time is then displayed in the HomeSafe error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

**Figure 32-6 Menu 24: System Maintenance**

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your HomeSafe as shown in the following screen.

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= NTP (RFC-1305)
Time Server Address= time-b.nist.gov

Current Time:                                08 : 07 : 14
New Time (hh:mm:ss):                        08 : 06 : 48

Current Date:                                2003 - 12 - 24
New Date (yyyy-mm-dd):                      2003 - 12 - 24

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):                          01 - 01
End Date (mm-dd):                            01 - 01

```

**Figure 32-7 Menu 24.10 System Maintenance: Time and Date Setting**

The following table describes the fields in this screen.

**Table 32-3 Time and Date Setting Fields**

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your timeserver sends when you turn on the HomeSafe. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. <b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server. <b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. <b>NTP (RFC-1305)</b> the default, is similar to <b>Time (RFC-868)</b> . <b>None</b> enter the time manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.

**Table 32-3 Time and Date Setting Fields**

<b>FIELD</b>	<b>DESCRIPTION</b>
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose <b>Yes</b> .
Start Date	Enter the month and day that your daylight-savings time starts on if you selected <b>Yes</b> in the <b>Daylight Saving</b> field.
End Date	Enter the month and day that your daylight-savings time ends on if you selected <b>Yes</b> in the <b>Daylight Saving</b> field.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

### 32.3.1 Resetting the Time

The HomeSafe resets the time in three instances:

- i. On leaving menu 24.10 after making changes.
- ii. When the HomeSafe starts up, if there is a timeserver configured in menu 24.10.
- iii. 24-hour intervals after starting.



# Chapter 33

## Remote Management

*This chapter covers remote management (SMT menu 24.11).*

### 33.1 Remote Management

Remote management allows you to determine which services/protocols can access which HomeSafe interface (if any) from which computers.

You may manage your HomeSafe from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable).



**When you Choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.**

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

Menu 24.11 - Remote Management Control

TELNET Server:	Port = 23	Access = LAN only
	Secure Client IP = 0.0.0.0	
FTP Server:	Port = 21	Access = LAN only
	Secure Client IP = 0.0.0.0	
Web Server:	Port = 80	Access = LAN only
	Secure Client IP = 0.0.0.0	
SNMP Service:	Port = 161	Access = LAN only
	Secure Client IP = 0.0.0.0	
DNS Service:	Port = 53	Access = LAN only
	Secure Client IP = 0.0.0.0	

**Figure 33-1 Menu 24.11 – Remote Management Control**

The following table describes the fields in this screen.

**Table 33-1 Menu 24.11 – Remote Management Control**

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service or protocol.	



**Table 33-1 Menu 24.11 – Remote Management Control**

FIELD	DESCRIPTION	EXAMPLE
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the HomeSafe.	23
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: <b>LAN only</b> , <b>WAN only</b> , <b>ALL</b> or <b>Disable</b> .	<b>LAN Only</b> (default)
Secure Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the HomeSafe. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

### 33.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the HomeSafe will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
6. There is a firewall rule that blocks it.

# Chapter 34

## Call Scheduling

*Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.*

### 34.1 Introduction to Call Scheduling

The call scheduling feature allows the HomeSafe to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Menu 26 - Schedule Setup

Schedule Set #	Name	Schedule Set #	Name
1		7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Schedule Set Number to Configure= 0


Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

**Figure 34-1 Menu 26 Schedule Setup**

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the HomeSafe, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.



**To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.**

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

```

Menu 26.1 - Schedule Set Setup

Active= Yes
Start Date(yyyy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
    Date(yyyy/mm/dd)= 2000 - 01 - 01
Weekdays:
    Sunday= N/A
    Monday= N/A
    Tuesday= N/A
    Wednesday= N/A
    Thursday= N/A
    Friday= N/A
    Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle

```

**Figure 34-2 Menu 26.1 Schedule Set Setup**

If a connection has been already established, your HomeSafe will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

**Table 34-1 Menu 26.1 Schedule Set Setup**

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to activate the schedule set.	<b>Yes</b>
Start Date	Enter the start date when you wish the set to take effect in year-month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select <b>Once</b> or <b>Weekly</b> . Both these options are mutually exclusive. If <b>Once</b> is selected, then all weekday settings are <b>N/A</b> . When <b>Once</b> is selected, the schedule rule deletes automatically after the scheduled time elapses.	<b>Once</b>
Once: Date	If you selected <b>Once</b> in the <b>How Often</b> field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday: Day	If you selected <b>Weekly</b> in the <b>How Often</b> field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select <b>Yes</b> , then press [ENTER].	<b>Yes</b> <b>No</b> <b>N/A</b>
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00

Table 34-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Action	<p><b>Forced On</b> means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the <b>Duration</b> field.</p> <p><b>Forced Down</b> means that the connection is blocked whether or not there is a demand call on the line.</p> <p><b>Enable Dial-On-Demand</b> means that this schedule permits a demand call on the line. <b>Disable Dial-On-Demand</b> means that this schedule prevents a demand call on the line.</p>	<b>Forced On</b>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP	Route= IP
Active= Yes	
Encapsulation= PPPoE	Edit IP= No
Service Type= Standard	Telco Option: _____
Service Name=	Allocated Budget (min)
Outgoing:	Period (hr)= 0
My Login=	Schedules= 1,2,3,4
My Password= *****	Nailed-Up Connection= No
Retype to Confirm= *****	
Authen= CHAP/PAP	
	Session Options:
	Edit Filter Sets= No
	Idle Timeout (sec)= 100
	Edit Traffic Redirect= No

Press ENTER to Confirm or ESC to Cancel:

Apply your  
schedule sets  
here

Figure 34-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

---

# Part IX:

---

## Appendices and Index

---

This section provides some Appendices and an Index.



# Appendix A

## Troubleshooting

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the HomeSafe.	Make sure that you have the correct power adapter connected to the HomeSafe and plugged in to an appropriate power source. Check all cable connections. If the LEDs still do not turn on, you may have a hardware problem. In this case, you should contact your local vendor.
Cannot access the HomeSafe from the LAN.	Check the cable connection between the HomeSafe and your computer or hub. Refer to the <i>Rear Panel</i> section for details. Ping the HomeSafe from a LAN computer. Make sure your computer Ethernet card is installed and functioning properly.
Cannot ping any computer on the LAN.	If the 10/100M LAN LEDs are off, check the cable connections between the HomeSafe and your LAN computers. Verify that the IP address and subnet mask of the HomeSafe and the LAN computers are in the same IP address range.
Cannot get a WAN IP address from the ISP.	The WAN IP is provided after the ISP verifies the MAC address, host name or user ID. Find out the verification method used by your ISP and configure the corresponding fields.
	If the ISP checks the WAN MAC address, you should clone the MAC address from a LAN computer. Click <b>WAN</b> and then the <b>MAC</b> tab, select <b>Spoof this Computer's MAC address - IP Address</b> and enter the IP address of the computer on the LAN whose MAC address you are cloning.
	If the ISP checks the host name, enter your computer's name (refer to the <i>Wizard Setup</i> section in the <i>User's Guide</i> ) in the <b>System Name</b> field in the first screen of the <b>WIZARD</b> .
	If the ISP checks the user ID, click <b>WAN</b> and then the <b>ISP</b> tab. Check your service type, user name, and password.
Cannot access the Internet.	Check the HomeSafe's connection to the cable/DSL device. Check whether your cable/DSL device requires a crossover or straight-through cable.
	Click <b>WAN</b> to verify your settings.
Access to a restricted web page is not blocked.	Make sure that the <b>Enable Parental Control</b> check box is selected in the <b>Parental Control</b> screen.
	When your content filtering subscription has expired, the <b>General</b> parental control screen displays <b>Not Registered</b> . Select the <b>Register Now</b> button to renew your content filtering subscription. Click <b>Register Now</b> to go to a web site where you can renew your category-based content filtering registration. You can use a trial application or register your iCard's PIN (you may have to purchase a new iCard to renew your subscription). Refer to the web site's on-line help for details.
	Make sure that the <b>Pre-defined Web Content Categories</b> check box is selected in the <b>Parental Control Group Edit</b> screen.
	Make sure that you select a blocked category in the <b>Parental Control Group Edit</b> screen to restrict access to web pages relevant to that category. For example, select the <b>Weapons</b> check box to prevent access to <a href="http://www.gun.com">www.gun.com</a> .

PROBLEM	CORRECTIVE ACTION
	Make sure that the <b>Time Scheduling</b> configured in the <b>Parental Control Edit</b> screen restricts access at the scheduled time.
Access to a web page with a URL containing a forbidden keyword is not blocked.	Make sure that you select the <b>Keyword Blocking</b> check box in the <b>Parental Control Group Edit</b> screen. Make sure that the keywords that you type are listed in the <b>Block Websites</b> list.
	If a keyword that is listed in the <b>Block Websites</b> list is not blocked when it is found in a URL, customize the keyword blocking using commands. See the <b>Customizing Keyword Blocking URL Checking</b> section in the <b>Parental Control</b> chapter.
Parental Control is configured correctly, but I can still access restricted web pages.	Restart the device to clear the cache.
	The content filter server may be unavailable. The <b>View Logs</b> screen can display content filtering log messages. See the <b>Log Descriptions</b> appendix for a list of possible log messages. In the <b>View Logs</b> screen copy and paste the log messages and e-mail them to customer support with an explanation of the problem.
	If you still have problems, contact your vendor or customer support for further advice.



# Appendix B

## PPPoE

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) that connects to an xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

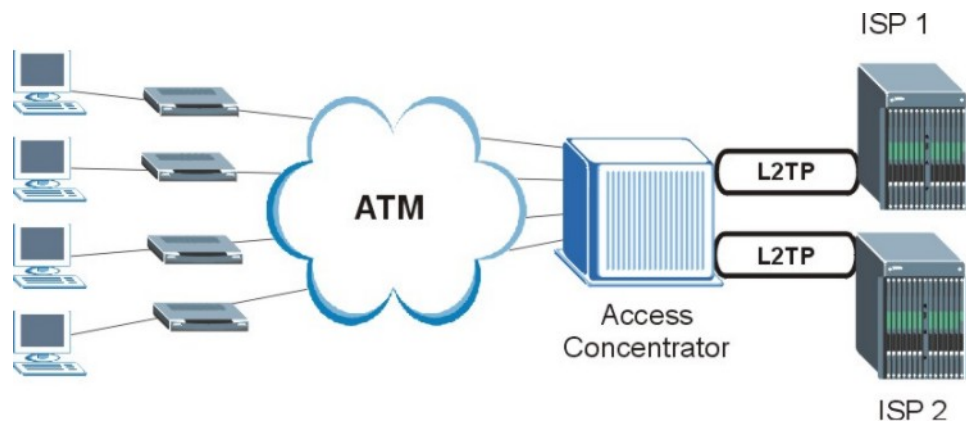
### Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

### Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.



**Diagram B-1 Single-PC per Modem Hardware Configuration**

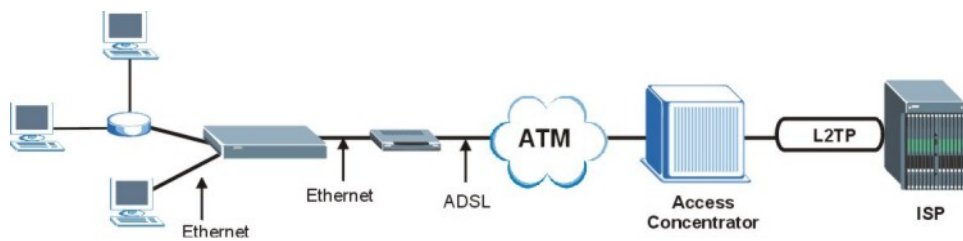
### How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

### **The HomeSafeas a PPPoE Client**

When using the HomeSafeas a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.



**Diagram B-2 The HomeSafeas a PPPoE Client**

# Appendix C

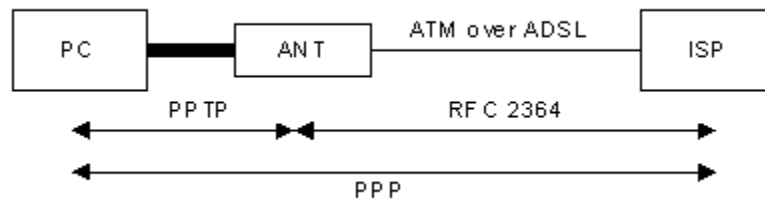
## PPTP

### What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

### How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.



**Diagram C-1 Transport PPP frames over Ethernet**

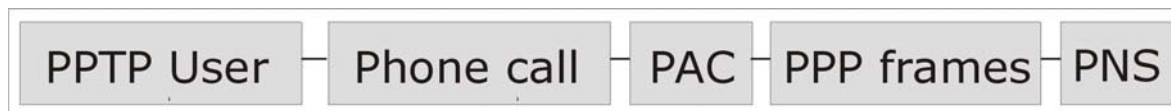
### PPTP and the HomeSafe

When the HomeSafe is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the HomeSafe's Internet connection. In NAT mode, the HomeSafe is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the PPTP connection is initialized by the remote PPTP Client, the user must configure the PPTP clients. The HomeSafe initializes the PPTP connection hence, there is no need to configure the remote PPTP clients.

## PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.



**Diagram C-2 PPTP Protocol Overview**

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the HomeSafe, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

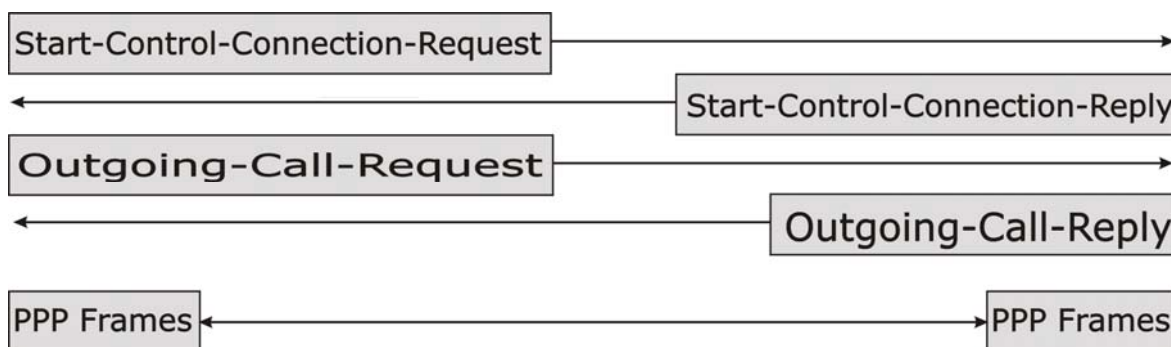
## Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

### Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.



**Diagram C-3 Example Message Exchange between PC and an ANT**

### PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.



# Appendix D

## Log Descriptions

*Configure centralized logs using the embedded web configurator; see the online help for details. This appendix describes some of the log messages.*

**Chart 1 System Error Logs**

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

**Chart 2 System Maintenance Logs**

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns	The DHCP server assigned an IP address to a client.
SMT Login Successfully	Someone has logged on to the router's SMT interface.
SMT Login Fail	Someone has failed to log on to the router's SMT interface.
WEB Login Successfully	Someone has logged on to the router's web configurator interface.
WEB Login Fail	Someone has failed to log on to the router's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via ftp.
FTP Login Fail	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
!! Phase 1 ID type mismatch	The ID type of an incoming packet does not match the local's peer ID type.
!! Phase 1 ID content	The ID content of an incoming packet does not match the local's peer

**Chart 2 System Maintenance Logs**

LOG MESSAGE	DESCRIPTION
mismatch	ID content.
!! No known phase 1 ID type found	The ID type of an incoming packet does not match any known ID type.

**Chart 3 UPnP Logs**

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

**Chart 4 Content Filtering Logs**

LOG MESSAGE	DESCRIPTION
URLFOR	The HomeSafe allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	The HomeSafe blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.
JAVBLK	The HomeSafe blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.
%s: Keyword blocking	The content of a requested web page matched a user-defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s: %s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s(cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s :%s(cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.



**Chart 4 Content Filtering Logs**

LOG MESSAGE	DESCRIPTION
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" checkbox, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The HomeSafe cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The HomeSafe cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

**Chart 5 ICMP Type and Code Explanations**

TYPE	CODE	DESCRIPTION
0	0	Echo Reply Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded

**Chart 5 ICMP Type and Code Explanations**

TYPE	CODE	DESCRIPTION
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

## Log Commands

Go to the command interpreter interface (Chapter 32 explains how to access and use the commands).

### Configuring What You Want the HomeSafe to Log

1. Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the HomeSafe is to record.
2. Use `sys logs category` to view a list of the log categories.

### Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
HS-100W> ?
Valid commands are:
sys          exit          device        ether
poe          pptp          config        wlan
ip           ppp           bridge       parentCtrl
radius       8021x
HS-100W>
```

3. Use `sys logs category` followed by a log category to display the parameters that are available for the category.

### Displaying Log Parameters Example

```
HS-100W> sys logs category access
```

Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/1:show debug type]

4. Use `sys logs category` followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

5. Use the `sys logs save` command to store the settings in the HomeSafe (you must do this in order to record logs).

### Displaying Logs

- Use the `sys logs display` command to show all of the logs in the HomeSafe's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual HomeSafe log category.
- Use the `sys logs clear` command to erase all of the HomeSafe's logs.

### Log Command Example

This example shows how to set the HomeSafe to record the access logs and alerts and then view the results.

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

```
HS-100W> sys logs load
HS-100W> sys logs category access 3
HS-100W> sys logs save
HS-100W> sys logs display access
```

#	.time message	source	destination	notes
0	01/01/2000 00:45:47   Successful SMT login			User:admin
1	01/01/2000 00:35:22   Successful SMT login			User:admin
2	01/01/2000 00:00:09   Successful SMT login			User:admin

```
HS-100W>
```



## Appendix E

# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

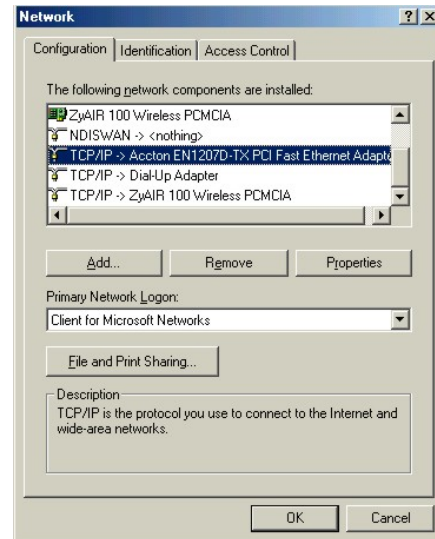
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet (192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0.) as the default HomeSafe's LAN port IP address (192.168.1.1).

### Windows 95/98/Me

1. Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window.



2. The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- In the **Network** window, click **Add**.
- Select **Adapter** and then click **Add**.
- Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- In the **Network** window, click **Add**.

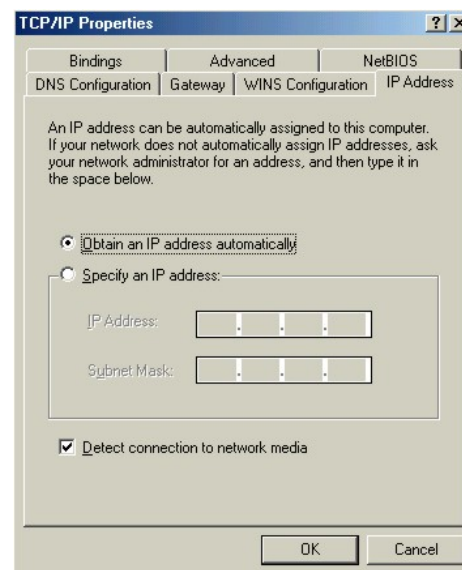
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

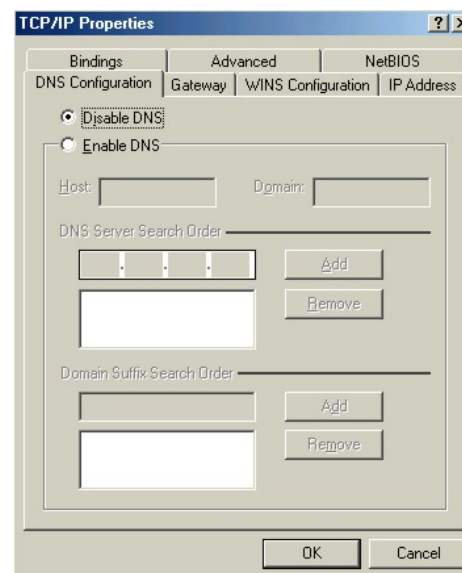
- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

1. Click the **IP Address** tab.  
 -To have your computer assigned a dynamic IP address, select **Obtain an IP address automatically**.  
 -To give your computer a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



2. Click the **DNS Configuration** tab.  
 -If you do not know your DNS information, select **Disable DNS**.  
 -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



3. Click the **Gateway** tab.

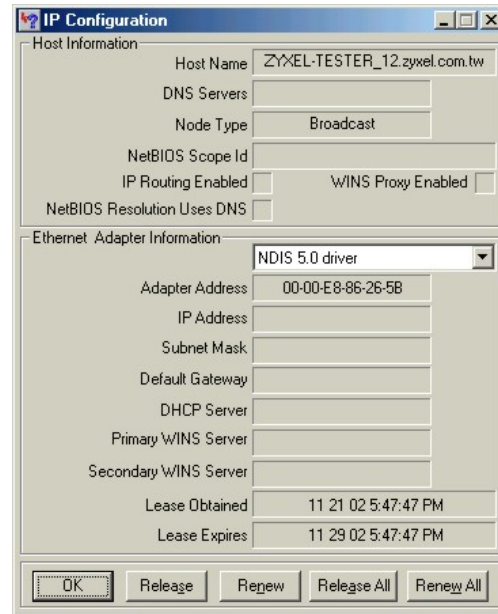


- If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
4. Click **OK** to save and close the **TCP/IP Properties** window.
  5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
  6. Turn on your HomeSafe and restart your computer when prompted.

### Checking/Modifying Your Computer's IP Address

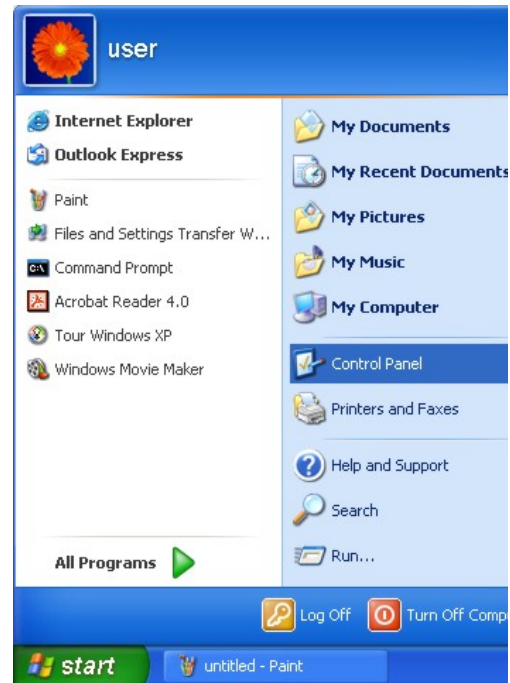
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's (static) IP address, subnet mask and default gateway in this screen. Verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default HomeSafeLAN IP address). Alternatively, to have the HomeSafe assign your computer a new IP address (from the IP pool), make sure your HomeSafe is turned on and click **Renew** in this screen.

Your computer can now communicate with the HomeSafe using the LAN port.

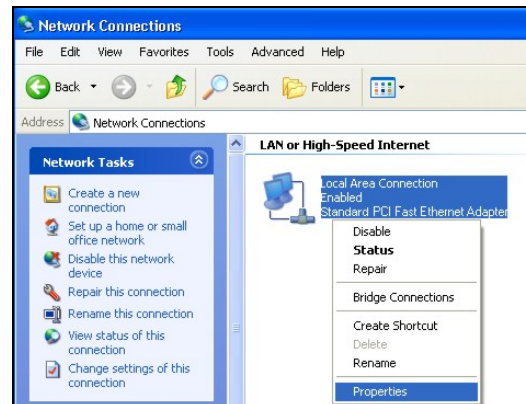


## Windows 2000/NT/XP

1. In Windows XP, click **start**, **Control Panel**.  
In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

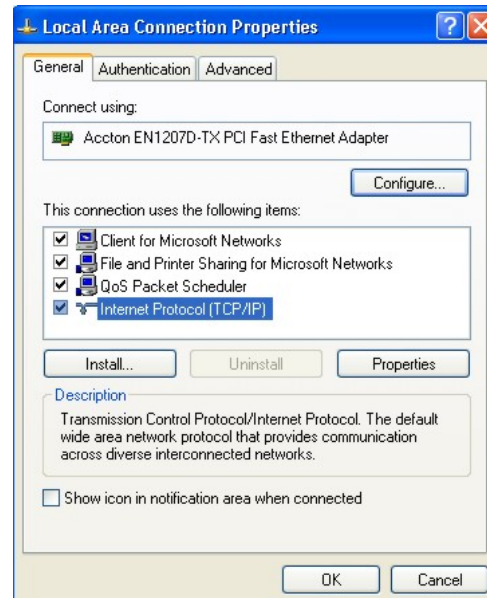


2. In Windows XP, click **Network Connections**.  
In Windows 2000/NT, click **Network and Dial-up Connections**.
3. Right-click **Local Area Connection** and then click **Properties**.

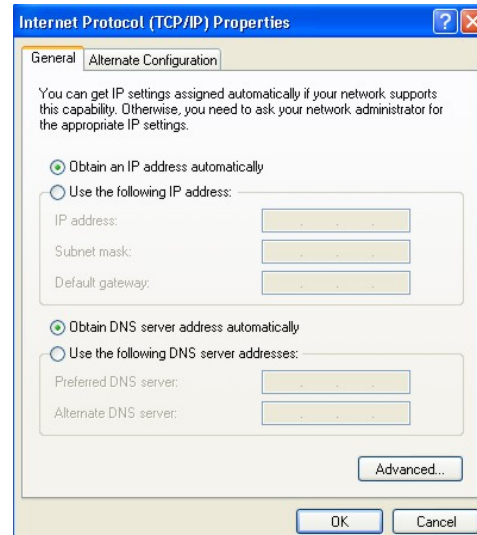




4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.



5. The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
  - To have your computer assigned a dynamic IP address, click **Obtain an IP address automatically**.
  - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.Click **Advanced** to go to the **Advanced TCP/IP Settings** screen shown next.



6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

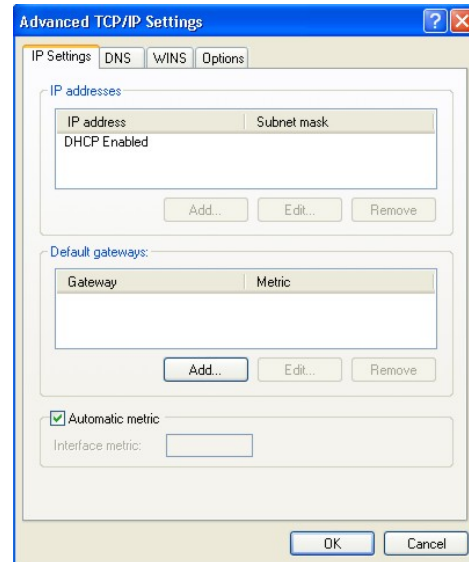
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

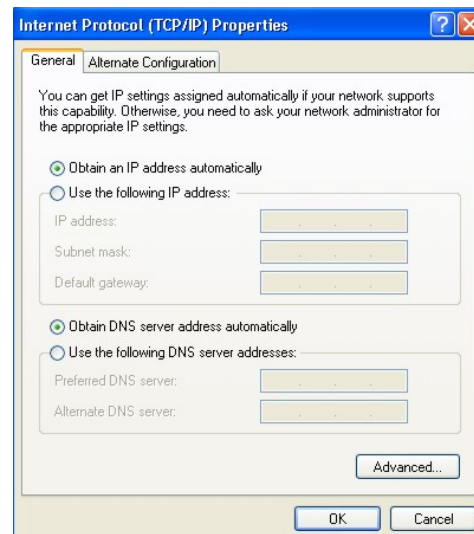


7. In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

-Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

-If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you wish to have more than two DNS servers, click **Advanced**, the **DNS** tab and then configure them using **Add**.



8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your HomeSafe and restart your computer (if prompted).

### Checking/Modifying Your Computer's IP Address

1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press **ENTER** to verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default HomeSafeLAN IP address). Alternatively, to have the HomeSafe assign your computer a new IP address (from the IP pool), make sure your HomeSafe is turned on, type "ipconfig/renew" and then press **ENTER**.

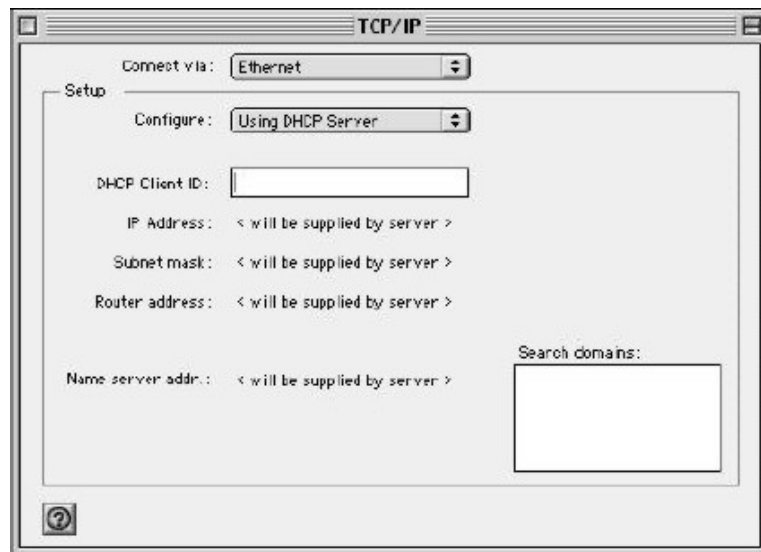
Your computer can now communicate with the HomeSafe using the LAN port.

## Macintosh OS 8/9

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.



2. Select **Ethernet built-in** from the **Connect via** list.



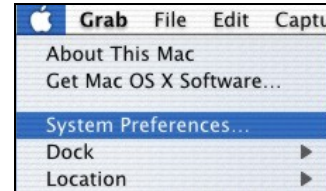
3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your HomeSafe in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your HomeSafe and restart your computer (if prompted).

## Verifying Your Computer's IP Address

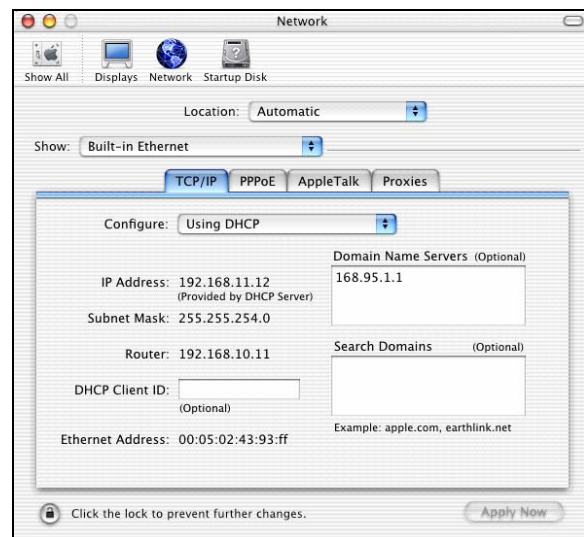
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

### Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.



2. Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.



3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.
4. For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your HomeSafein the **Router address** box.
5. Click **Apply Now** and close the window.
6. Turn on your HomeSafeand restart your computer (if prompted).

## Verifying Your Computer's IP Address

Check your TCP/IP properties in the **Network** window.



# Appendix F

## Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

### Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

### IEEE 802.11

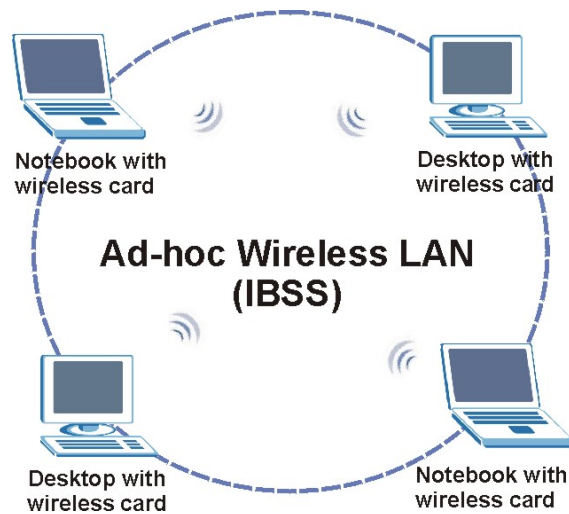
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any

time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.



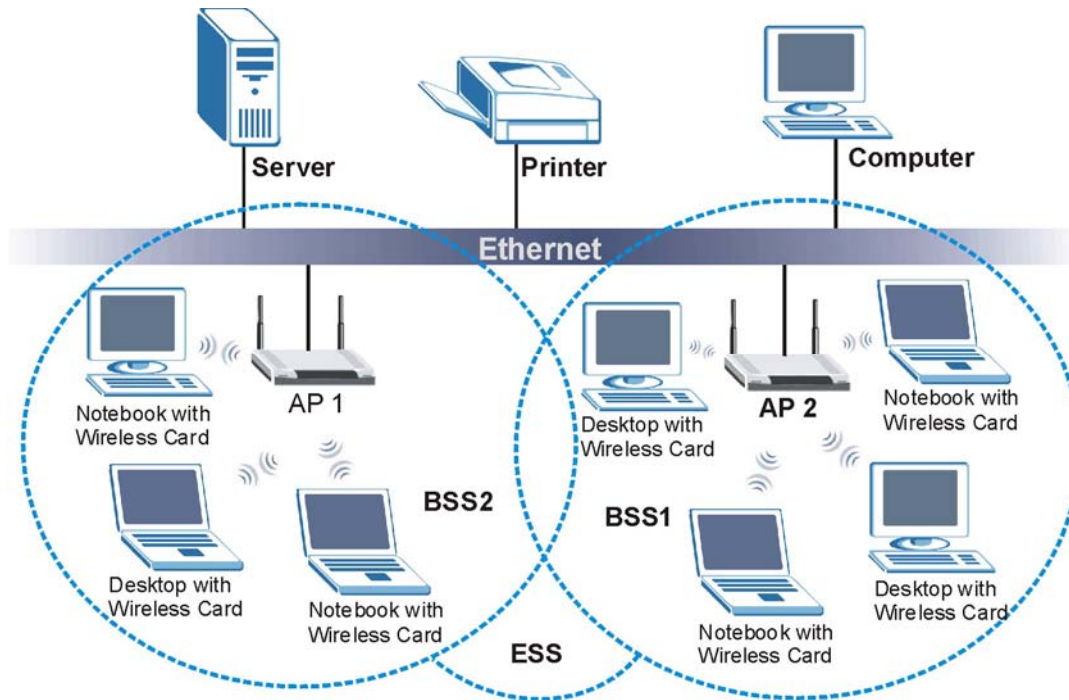
**Diagram F-1 Peer-to-Peer Communication in an Ad-hoc Network**

## Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.





**Diagram F-2 ESS Provides Campus-Wide Coverage**



# Appendix G

## Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

### Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

### Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

### IEEE 802.1x

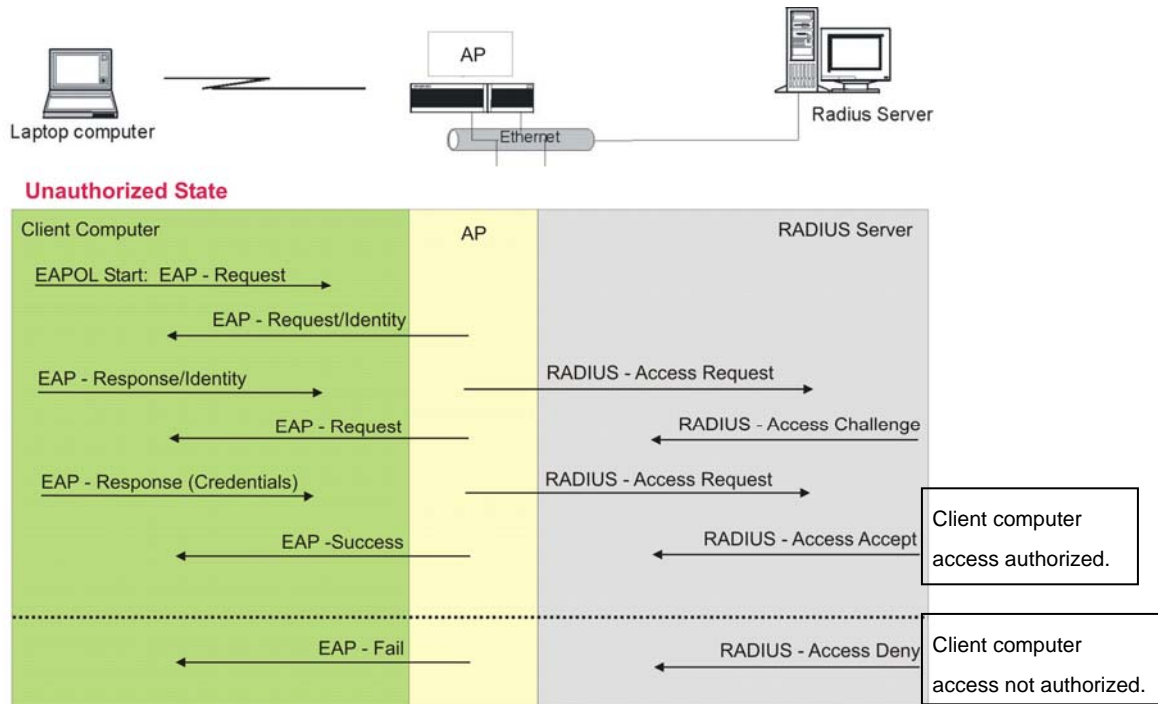
In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

### Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

#### RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).



**Diagram G-1 Sequences for EAP MD5-Challenge Authentication**

## Appendix H

# Types of EAP Authentication

This appendix discusses the four popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS** and **PEAP**. The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5 and EAP-MSCHAPv2, for client authentication.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, simple user name and password pair is more practical. The following table is a comparison of the features of four authentication types.

**Comparison of EAP Authentication Types**

	<b>EAP-MD5</b>	<b>EAP-TLS</b>	<b>EAP-TTLS</b>	<b>PEAP</b>
<b>Mutual Authentication</b>	No	Yes	Yes	Yes

**Comparison of EAP Authentication Types**

	<b>EAP-MD5</b>	<b>EAP-TLS</b>	<b>EAP-TTLS</b>	<b>PEAP</b>
<b>Certificate – Client</b>	No	Yes	Optional	Optional
<b>Certificate – Server</b>	No	Yes	Yes	Yes
<b>Dynamic Key Exchange</b>	No	Yes	Yes	Yes
<b>Credential Security</b>	None	Strong	Strong	Strong
<b>Deployment Difficulty</b>	Easy	Hard	Moderate	Moderate
<b>Wireless Security</b>	Poor	Best	Good	Good
<b>Client Identity Protection</b>	No	No	Yes	Yes

# Appendix I

## Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

### Antenna Characteristics

#### ➤ Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

#### ➤ Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

#### ➤ Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

### Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

## **Positioning Antennas**

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.



# Appendix J

## Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See other *appendices* for information on the command structure.

**Chart 6 Brute-Force Password Guessing Protection Commands**

COMMAND	DESCRIPTION
<code>sys pwderrrtm</code>	This command displays the brute-force guessing password protection settings.
<code>sys pwderrrtm 0</code>	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
<code>sys pwderrrtm N</code>	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

### Example

<code>sys pwderrrtm 5</code>	This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.
------------------------------	--



# Appendix K

## Triangle Route

### The Ideal Setup

When the firewall is on, your HomeSafe acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the HomeSafe to protect your LAN against attacks.

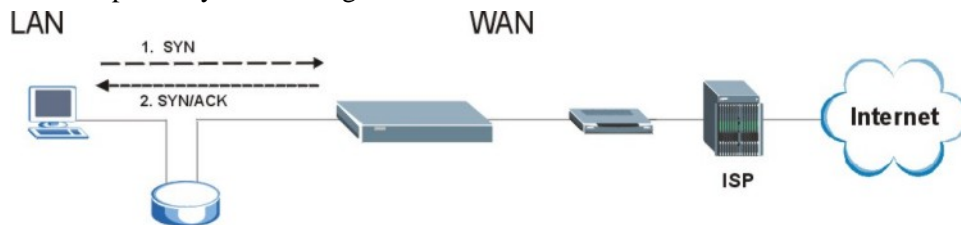


Diagram K-1 Ideal Setup

### The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

- Step 1.** A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- Step 2.** The HomeSafe routes the SYN packet through Gateway **B** on the LAN to the WAN.
- Step 3.** The reply from the WAN goes directly to the computer on the LAN without going through the HomeSafe.

As a result, the HomeSafe resets the connection, as the connection has not been acknowledged.

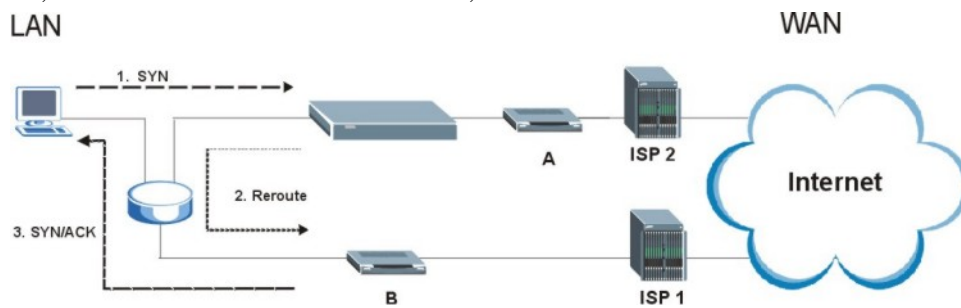


Diagram K-2 “Triangle Route” Problem

### The “Triangle Route” Solutions

This section presents you two solutions to the “triangle route” problem.

#### IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your HomeSafe supports up to three logical LAN interfaces with the HomeSafe being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the HomeSafe to your LAN. The following steps describe such a scenario.

- Step 1.** A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- Step 2.** The HomeSafe reroutes the packet to Gateway **B** which is in Subnet 2.
- Step 3.** The reply from WAN goes through the HomeSafe to the computer on the LAN in Subnet 1.

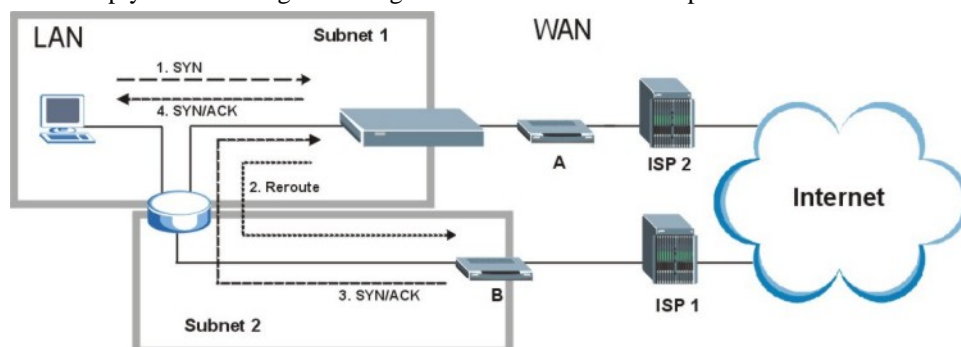


Diagram K-3 IP Alias

## Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your HomeSafe to your LAN. Therefore your LAN is protected.

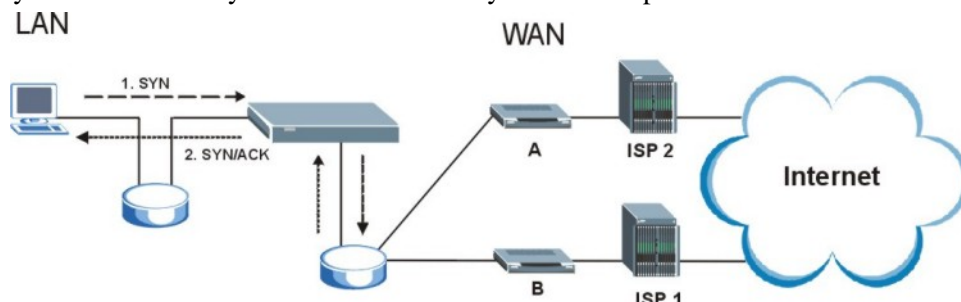


Diagram K-4 Gateways on the WAN Side

## How To Configure Triangle Route:

- Step 1.** From the SMT main menu, enter 24.
- Step 2.** Enter “8” in menu 24 to enter CI command mode.
- Step 3.** Use the following commands to allow/disallow triangle route.

<code>sys firewall ignore triangle all off</code>	This command allows triangle route.
<code>sys firewall ignore triangle all on</code>	This command disallows triangle route.

# Appendix L

## Index

**8**  
802.1x ..... 7-11

**A**  
Active ..... 22-2  
Address Assignment ..... 3-8, 3-9  
Address Resolution Protocol (ARP) ..... 5-3  
Ad-hoc Configuration ..... F-1  
Allocated Budget ..... 22-4  
Antenna  
    Directional ..... I-2  
    Omni-directional ..... I-1  
    Types ..... I-1  
Antenna gain ..... I-1  
Applications ..... 1-5  
AT command ..... 31-1  
Authen ..... 22-4  
Authentication ..... 7-3, 22-3, 22-4  
Authentication Protocol ..... 22-3  
auto-negotiation ..... 1-1

**B**  
Backup ..... 16-7, 31-2  
Basic Service Set ..... F-1  
Bridging ..... 20-1  
BSS ..... 6-1. *See* Basic Service Set  
Budget Management ..... 32-2

**C**  
CA ..... H-1  
Call Control ..... 32-2  
Call History ..... 32-3  
Call Scheduling ..... 1-3, 34-1  
    Maximum Number of Schedule Sets ..... 34-1  
    PPPoE ..... 34-3  
    Precedence ..... 34-1  
    Precedence Example ..... *See* precedence  
Call-Triggerring Packet ..... 30-6  
Canada ..... iv  
Caution ..... iv  
CDR (Call Detail Record) ..... 30-4  
Certificate Authority ..... *See* CA  
Channel ID ..... 6-5, 20-6  
CHAP ..... 22-4  
Command Interpreter Mode ..... 32-1  
Community ..... 28-2  
Computer Name ..... 18-1

Computer's IP Address ..... E-1  
Conditions that prevent TFTP and FTP from  
    working over WAN ..... 31-3  
Configuration ..... 5-1, 16-3  
Connection ID/Name ..... 22-5  
Content Filtering ..... 1-2  
Copyright ..... ii  
Cost Of Transmission ..... 23-2  
Customer Support ..... vi

**D**  
Data Encryption ..... 7-3  
DDNS Type ..... 18-3  
Default ..... 16-8  
Denial of Service ..... 26-1  
DHCP .... 3-1, 3-9, 4-2, 5-1, 5-4, 16-3, 20-2, 30-3  
DHCP (Dynamic Host Configuration Protocol) 1-4  
Diagnostic Tools ..... 30-1  
Direct Sequence Spread Spectrum ..... F-1  
Disclaimer ..... ii  
Distribution System ..... F-2  
DNS ..... 14-9, 20-3  
Domain Name ..... 3-1, 3-9, 9-5, 30-2  
DoS (Denial of Service) ..... 1-2  
DS ..... *See* Distribution System  
DSL Modem ..... 1-5, 22-3  
DSSS ..... *See* Direct Sequence Spread Spectrum  
Dynamic DNS ..... 4-2, 18-2  
Dynamic DNS Support ..... 1-3  
Dynamic WEP Key Exchange ..... 7-12  
DYNDNS Wildcard ..... 4-2

**E**  
e.g. .... *See* Syntax Conventions  
EAP ..... 1-2  
EAP Authentication ..... H-1, 7-21  
    MD5 ..... H-1  
    TLS ..... H-1  
    TTLS ..... H-1  
ECHO ..... 9-5  
Edit IP ..... 22-2  
Enable Wildcard ..... 18-3  
Encapsulation ..... 21-1, 22-2, 22-5  
    PPP over Ethernet ..... B-1  
Encryption ..... 7-6  
Enter ..... *See* Syntax Conventions  
ESS ..... 6-2. *See* Extended Service Set.  
Ethernet ..... 3-4, 3-5, 13-1

Ethernet Encapsulation.....9-5, 21-1, 22-1, 22-7  
 Extended Service Set.....F-2, 6-2  
 Extended Service Set IDentification..... 6-5

## F

Factory Default..... 19-1  
 Factory LAN Defaults ..... 5-1  
 Fail Tolerance..... 22-8  
 FCC ..... iii  
 FHSS .*See* Frequency-Hopping Spread Spectrum  
 Filename Conventions ..... 31-1  
 Filter ..... 20-1, 22-7  
     Applying ..... 27-12  
     Configuring ..... 27-3  
     Example ..... 27-9  
     Generic Filter Rule..... 27-7  
     Generic Rule ..... 27-8  
     NAT ..... 27-11  
     Remote Node..... 27-12  
     Structure..... 27-1  
     TCP/IP Rule ..... 27-5  
 Filters  
     Executing a Filter Rule..... 27-2  
     IP Filter Logic Flow ..... 27-6  
 Finger ..... 9-5  
 Firewall..... 1-2, 13-1  
     Access Methods ..... 26-1  
     Remote Management ..... 26-1  
     Services..... 12-13  
     SMT Menus ..... 26-1  
 Firmware File  
     *Maintenance*..... 16-5, 16-6  
 Fragment Threshold..... 20-6  
 Fragmentation Threshold..... 6-4  
 Frequency-Hopping Spread Spectrum..... F-1  
 FTP..... 4-2, 5-1, 9-4, 9-5, 13-1, 14-1, 14-4, 33-2  
 FTP File Transfer ..... 31-6  
 FTP Restrictions ..... 14-1, 31-3, 33-2  
 FTP Server..... 1-4, 25-9  
 Full Network Management..... 1-4

## G

Gateway..... 23-2  
 Gateway IP Addr ..... 22-5  
 Gateway IP Address ..... 21-2  
 General Setup ..... 3-1, 4-1, 18-1  
 Global ..... 9-1

## H

Hidden Menus ..... 17-2  
 Hop Count ..... 23-2  
 Host ..... 4-4, 18-3  
 How PPPoE Works ..... B-1  
 HTTP ..... 9-5

## I

i.e. .... *See* Syntax Conventions  
 IBSS..... 6-1. *See* Independent Basic Service Set  
 Idle Timeout ..... 22-3, 22-4  
 IEEE 802.11 ..... F-1  
     Deployment Issues ..... G-1  
     Security Flaws..... G-1  
 IEEE 802.1x ..... G-1, 1-2  
     Advantages..... G-1  
 IGMP ..... 5-2  
 Incoming Protocol Filters ..... 20-5  
 Independent Basic Service Set..... F-2, 6-1  
 Industry Canada..... iv  
 Infrastructure Configuration ..... F-2  
 Inside ..... 9-1  
 Inside Global Address ..... 9-1  
 Inside Local Address ..... 9-1  
 Internet access ..... 21-1  
 Internet Access ..... 20-1, 21-1  
     ISP's Name ..... 21-1  
 Internet Access Setup ..... 21-1, 25-1  
 Internet Security Gateway ..... 1-1  
 Introduction to Filters ..... 27-1  
 IP Address 3-8, 3-9, 5-1, 5-5, 9-5, 9-6, 9-7, 16-3,  
     20-3, 20-5, 21-2, 22-5, 23-1, 30-3  
 IP Address Assignment ..... 22-5  
 IP Address Assignment ..... 21-2  
 IP Alias ..... 1-3, 20-5  
 IP Alias Setup ..... 20-4  
 IP Multicast ..... 1-3  
     Internet Group Management Protocol (IGMP)  
         ..... 1-3  
 IP Pool ..... 5-4, 20-2  
 IP Pool Setup ..... 5-1  
 IP Static Route ..... 23-1  
 IP Static Route Setup..... 23-1  
 IP Subnet Mask..... 20-5  
 ISP's Name ..... 21-1

## L

LAN Setup..... 5-1, 8-1  
 LAN TCP/IP ..... 5-1  
 Local ..... 9-1  
 Local User Database..... 7-19  
 Log Facility ..... 30-4  
 Logging ..... 1-4  
 Login Name ..... *See* My Login Name

## M

MAC Address ..... 19-1  
 MAC Address Filter Action..... 7-18, 20-8  
 MAC Address Filtering ..... 7-17, 20-7  
 MAC Filter ..... 7-17  
 Main Menu ..... 17-3

Management Information Base (MIB) 14-6, 28-1  
 Many to Many No Overload..... *See* NAT  
 Many to Many Overload ..... *See* NAT  
 Many to One ..... *See* NAT  
 MD5 ..... H-1  
 Message Digest Algorithm 5 ..... *See* MD5  
 Message Logging ..... 30-4  
 Metric ..... 8-1, 10-3, 22-6, 23-2  
 Multicast..... 5-2, 5-5, 20-3, 22-6  
 My IP Addr..... 22-5  
 My Login..... 22-2  
 My Login Name ..... 21-1  
 My Password ..... 21-1, 22-2  
 My Server IP Addr ..... 22-5

## N

Nailed-up Connection..... 22-3  
 Nailed-Up Connection..... 22-4  
 NAT..... 2-5, 3-6, 9-4, 9-5, 9-6, 9-7, 22-6, 27-11  
     Applying NAT in the SMT Menus ..... 25-1  
     Configuring ..... 25-2  
     Definitions..... 9-1  
     Examples..... 25-7  
     How NAT Works ..... 9-2  
     Mapping Types ..... 9-3  
     Non NAT Friendly Application Programs . 25-11  
     Ordering Rules ..... 25-4  
     Server Sets ..... 9-5  
     What NAT does ..... 9-1  
 NAT Traversal..... 11-1, 11-2  
 Navigation Panel ..... 2-21  
 Network Address Translation ..... 21-2  
 Network Address Translation (NAT) .... 1-4, 25-1  
 Network Management ..... 9-5  
 Network Topology With RADIUS Server  
     Example ..... G-1  
 NNTP ..... 9-5  
 Notice ..... iii

## O

Offline ..... 18-3  
 One to One..... *See* NAT  
 Online Registration..... v  
 Outgoing Protocol Filters ..... 20-5  
 Outside ..... 9-1

## P

Packet Filtering..... 1-3  
 Packing List Card ..... xxii  
 PAP..... 22-4  
 Parental Control..... 12-1  
 Password4-4, 17-1, 17-4, 28-2. *See* My Password  
 Period(hr) ..... 22-4

Ping..... 30-7  
 Point-to-Point Tunneling Protocol... 3-7, 9-5. *See* PPTP  
 POP3..... 9-5  
 Port Forwarding ..... 1-4  
 Port Numbers ..... 9-5  
 PPPoE ..... 1-3, 2-5, 3-4, 3-5, 3-6  
 PPPoE Encapsulation 21-1, 21-3, 22-1, 22-3, 22-4  
 PPTP ..... 3-4, 3-6, 3-7, 9-5  
     Client..... 21-2, 21-3  
     Configuring a Client..... 21-2, 21-3  
 PPTP and the Prestige..... C-1  
 PPTP Encapsulation ..... 1-3, 3-7, 22-4  
 PPTP Protocol Overview ..... C-2  
 PPTP, What is it?..... C-1  
 Preamble Mode..... 7-4  
 Prestige as a PPPoE Client ..... B-2  
 Private..... 10-3, 22-6, 23-2  
 Private IP Address ..... 3-8  
 Protocol Filters ..... 20-5  
     Incoming ..... 20-5  
     Outgoing..... 20-5

## Q

Quick Start Guide ..... 2-1

## R

RADIUS ..... 1-2, 7-20  
 RAS ..... 30-3  
 Related Documentation ..... xxii  
 Relay..... 20-2  
 Rem Node Name ..... 22-2  
 Remote Authentication Dial In User Service.. *See* RADIUS  
 Remote Management  
     Firewall ..... 26-1  
 Remote Management and NAT ..... 14-2  
 Remote Management Limitations..... 14-1, 33-2  
 Remote Node ..... 22-1  
 Remote Node Filter ..... 22-6  
 Remote Node Traffic ..... 27-13  
 Repairs..... v  
 Replacement ..... v  
 Required fields..... 17-3  
 Reset Button ..... 1-1  
 Resetting the Time..... 32-5  
 Restore ..... 16-7  
 Restore Configuration..... 31-4  
 Return Material Authorization Number..... v  
 RF signals ..... F-1  
 RIP..... 5-1, 5-2, 20-3, 20-5, 22-6  
     Direction..... 20-5  
     Version ..... 20-5, 22-6  
 RoadRunner Support ..... 1-4

Roaming .....	6-5
Enable on ZyAIR .....	20-8
Example .....	6-6
Requirements .....	6-6
Route .....	22-2
RTC .....	<i>See</i> Real Time Chip
RTS Threshold .....	6-3, 20-6
Rules	
Predefined Services .....	12-13

## S

Schedule Sets	
Duration .....	34-2
Schedules .....	22-4
Security Parameters .....	7-3
Select .....	<i>See</i> Syntax Conventions
Server 4-5, 9-3, 9-4, 21-1, 21-2, 22-2, 25-2, 25-4, 25-5, 25-6, 25-8, 32-4	
Server IP .....	22-2
Service .....	v
Service Name .....	22-4
Service Set .....	6-5
Service Type .....	21-1, 22-2
Services .....	9-5, 13-4
setup a schedule .....	34-1
SMT Menu Overview .....	17-1
SMTP .....	9-5
SNMP .....	9-5, 13-2, 14-5
Community .....	28-2
Configuration .....	28-2
Get .....	14-6, 28-1
Manager .....	14-6, 28-1
MIBs .....	14-7, 28-2
Trap .....	14-6, 28-2
Trusted Host .....	28-2
SNMP ( Simple Network Management Protocol) .....	1-3
Stateful Inspection .....	1-2, 13-1
Static Route .....	10-1
SUA .....	9-4, 9-5, 9-6, 9-7
SUA (Single User Account) .	<i>See</i> NAT. <i>See</i> NAT
Subnet Mask ..	3-9, 5-1, 5-5, 20-3, 21-2, 22-5, 23-2, 30-3
Support Disk .....	xxii
Syntax Conventions .....	xxiii
Syslog .....	30-4
Syslog IP Address .....	30-4
Syslog Server .....	30-4
System	
Console Port Speed .....	30-4
Diagnostic .....	30-6
Log and Trace .....	30-4
Syslog and Accounting .....	30-4
System Information .....	30-3
System Status .....	30-1

System Information .....	30-3
System Information & Diagnosis .....	30-1
System Maintenance	15-1, 30-1, 30-2, 30-3, 30-7, 31-2, 31-3, 31-7, 32-1, 32-2, 32-3, 32-4
System Management Terminal .....	17-2
System Name .....	4-1, 18-1
System Status .....	30-2
System Timeout .....	14-2

## T

TCP/IP ....	5-5, 14-3, 20-3, 22-5, 27-4, 27-5, 27-6, 27-8, 27-11
Setup .....	20-3
TCP/IP filter rule .....	27-4
Telnet .....	14-3
Telnet Configuration .....	14-3
TFTP and FTP over WAN Management	
Limitations .....	31-3
TFTP and FTP Over WAN} .....	14-1, 33-2
TFTP File Transfer .....	31-7
TFTP Restrictions .....	14-1, 31-3, 33-2
Time and Date .....	1-1
Time and Date Setting .....	32-4
Time Setting .....	4-4
Time Zone .....	32-5
Timeout .....	21-3, 21-4, 22-4
TLS .....	H-1
Trace Records .....	30-4
Tracing .....	1-4
Trademarks .....	ii
Traffic Redirect .....	1-4, 8-9
Setup .....	22-7
Transport Layer Security .....	<i>See</i> TLS
Triangle .....	K-1
Triangle Route\ Solutions .....	K-1
Trigger Port Forwarding .....	25-12
Process .....	9-10
TTLS .....	H-1
Tunneled Transport Layer Service .....	<i>See</i> TTLS

## U

Universal Plug and Play .....	1-3
Universal Plug and Play (UPnP) .....	11-1, 11-2
UNIX Syslog .....	30-4
UNIX syslog parameters .....	30-4
Upload Firmware .....	31-5
UPnP .....	1-3
UPnP Examples .....	11-2
Use Server Detected IP .....	18-4
User Authentication .....	7-6
User Name .....	4-3, 18-3
User Profiles .....	7-19, 24-1
User Specified IP Addr .....	18-4



<b>V</b>	
VPN .....	8-4
<b>W</b>	
WAN DHCP .....	30-7
WAN Setup .....	3-9, 19-1
Warranty .....	v
Web .....	14-2
Web Configurator .....	2-1, 2-20, 26-1
WEP .....	7-3
WEP Encryption .....	7-5, 7-8, 20-6
What is PPTP? .....	C-1
Wireless Client WPA Supplicants .....	7-9
Wireless LAN .....	F-1, 20-5
<b>Z</b>	
Benefits .....	F-1
Wireless LAN Setup .....	20-5
Wireless Security .....	7-1
Wizard Setup .....	3-1, 3-2, 3-3, 3-8
WLAN .....	<i>See</i> Wireless LAN
WPA .....	7-6
WPA with RADIUS Application .....	7-9
WPA-PSK Application .....	7-7
www.dyndns.org .....	18-3
<b>Z</b>	
ZyNOS .....	30-2, 31-1
ZyNOS F/W Version .....	30-2, 31-1
ZyXEL Limited Warranty	
Note .....	v